McGeorge Law Review

Volume 46 | Issue 3 Article 4

1-1-2014

The Changing Face of Espionage: Modern Times Call for Amending the Espionage Act

Lindsay B. Barnes
Pacific McGeorge School of Law

Comments

The Changing Face of Espionage: Modern Times Call for Amending the Espionage Act

Lindsay B. Barnes*

TABLE OF CONTENTS

"I urge you to enact [espionage] laws at the earliest possible moment and feel that in doing so I am urging you to do nothing less than save the honor and self-respect of the nation. Such creatures of passion, disloyalty, and anarchy must be crushed out."

—President Woodrow Wilson[1]

I. INTRODUCTION

In May 2013, *The Guardian* published a series of stories detailing Top Secret United States surveillance programs.[2] A week later, Edward Snowden, a former government contractor for the National Security Agency (NSA), revealed to the world that he was the source.[3] Upon this disclosure, he sought asylum abroad for his actions, and for good reason.[4] Less than a month later, he was formally charged with two counts under the Espionage Act of 1917,[5] among other crimes.[6] The charges came only a month before the conviction of former United States Army private Bradley Manning, who was found guilty on six counts under the Espionage Act for providing thousands of classified military-related documents and videos to Wikileaks for publication.[7]

The United States Government's use of the Espionage Act to condemn Snowden's and Manning's actions[8] has called into question the adequacy of the

---

* J.D. Candidate, University of the Pacific, McGeorge School of Law, 2015; B.A., University of Nevada, Reno, 2008. I would like to thank Professor John Sims for his invaluable guidance and assistance in writing this Comment. I would also like to thank the *McGeorge Law Review* editors and my family and friends for their incredible support.

1. THIRD ANNUAL MESSAGE FROM PRESIDENT WILSON TO CONGRESS, Dec. 7, 1915, in 53 CONG. REC. 99 (1915) [*hereinafter* THIRD ANNUAL MESSAGE].

2. Glenn Greenwald et al., *Edward Snowden: The Whistleblower Behind the NSA Surveillance Revelations*, THE GUARDIAN (June 9, 2013), www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance (on file with the *McGeorge Law Review*).

3. *Id*.

4. Peter Baker & Ellen Barry, *Snowden, in Russia, Seeks Asylum in Ecuador*, N.Y. TIMES (June 23, 2013), www.nytimes.com/2013/06/24/world/asia/nsa-leaker-leaves-hong-kong-local-officials-say.html?pagewanted=all (on file with the *McGeorge Law Review*).

5. 18 U.S.C. §§ 792–798 (2012).

6. Criminal Complaint, United States v. Snowden, No. 1:13 CR 265 (E.D.Va. June 14, 2013) (charging Snowden under sections 793(d) and 798(a)(3) of the Espionage Act and a charge for theft of government property under 18 U.S.C. § 641).

7. Charlie Savage, *Manning is Acquitted of Aiding the Enemy*, N.Y. TIMES (July 30, 2013), www.nytimes.com/2013/07/31/us/bradley-manning-verdict.html?pagewanted%253Dall (on file with the *McGeorge Law Review*) (noting that the military court found Manning guilty on six counts in violation of the Espionage Act, but found him not guilty on the charge of "aiding the enemy" under Article 104 of the Uniform Code of Military Justice). Bradley Manning is now called Chelsea Manning after announcing that he identifies himself as female shortly after his conviction. Michael Pearson, *Bradley Manning Wants to Live as a Woman, be Known as Chelsea*, CNN (Aug. 23, 2013, 6:45 AM), http://www.cnn.com/2013/08/22/us/bradley-manning (on file with the *McGeorge Law Review*). This Comment uses the name Bradley Manning as he was known during the time the events addressed transpired.

8. Lincoln Caplan, *Leaks and Consequences*, AM. SCHOLAR, Autumn 2013, *available at* http://theamericanscholar.org/leaks-and-consequences/#.UknLcoakpHQ/utm_source=pbkemail (on file with the

antique statute.[9] Neither the 64th or the 65th Congress specifically contemplated modern disclosures of protected information that could fall within the provisions of the Espionage Act, such as improper whistleblowing[10] and other unauthorized leaks.[11] Rather, Congress intended the Act to solve grave wartime concerns, like spying and disloyal conduct, that disrupted military efforts.[12] Notwithstanding various criticisms and a few early amendments,[13] the Espionage Act remains staunchly similar to the original language of 1917.[14]

While the Espionage Act endures, scholars, judges, and government officials have criticized the statute for its ambiguity and overbreadth.[15] These concerns have led to increased scrutiny of the Espionage Act, especially in the wake of Snowden's public disclosure of Top Secret government surveillance programs

---

McGeorge Law Review).

9. Elizabeth Goitein, *Our Antiquated Laws Can't Cope with National Security Leaks*, TIME (June 12, 2013), https:// ideas.time.com/2013/06/12/our-antiquated-laws-cant-cope-with-national-security-leaks (on file with the *McGeorge Law Review*).

10. A whistleblower is generally defined as "[a]n employee who reports employer wrong doing to a governmental or law-enforcement agency." BLACK'S LAW DICTIONARY 1831 (10th ed. 2014).

11. *See infra* Part II.A (discussing the history of the Espionage Act); *see also* Caplan, *supra* note 8 (noting that "reinterpretation of the statute has led the government to equate leakers with spies"). Unauthorized leaks are contrasted with leaks that are either authorized or executed on a routine basis, and such leakers are not charged under the Espionage Act. Steven Aftergood, *Some Unauthorized Disclosures of Classified Info are Routine,* SECRECY NEWS (June 11, 2012), http://blogs.fas.org/secrecy/2012/06/routine_leaks (on file with the *McGeorge Law Review*) [hereinafter Aftergood, *Some Unauthorized Disclosures*] ("[T]he peculiar reality is that certain officials routinely take it upon themselves to discuss classified information with unauthorized persons."). It has been suggested that some government employees who have leaked information consistent with popular government policy have received no reprimand or penalty, whereas government employees who leak information inconsistent with government policy face potential espionage charges. *See e.g.* Robert Naiman, *Amend or Repeal the Espionage Act to Protect Journalists and Whistle-blowers*, HUFFINGTON POST (Aug. 15, 2013, 9:08 AM), http://www.huffingtonpost. com/robert-naiman/amend-or-repeal-theespio_b_3756527.html (on file with the *McGeorge Law Review*) (explaining "[The Espionage Act] allows selective prosecution of whistle-blowers on an extreme charge.").

12. *See* Geoffrey R. Stone, *Judge Learned Hand and the Espionage Act of 1917: A Mystery Unraveled*, 70 U. CHI. L. REV. 335, 336, 352 (2003) (referencing in part DAVID M. KENNEDY, OVER HERE: THE FIRST WORLD WAR AND AMERICAN SOCIETY 24 (Oxford, 25th ed. 2004) regarding Woodrow Wilson's Third Annual Message to Congress) ("[A]s early as 1916, in his third annual message to Congress, President Wilson 'cited the need for legislation to suppress disloyal activities.'"); Alan Rozenshtein, *An Explainer on the Espionage Act and the Third-Party Leak Prosecutions*, LAWFARE (May 22, 2013, 1:00 PM), www.lawfairblog.com/2013/ 05/an-explainer-on-the-espionage-act-and-the-third-party-leak-prosecutions (on file with the *McGeorge Law Review*) (explaining that the Espionage Act was enacted to stop attempts to thwart U.S. war efforts).

13. *See* Robert D. Epstein, *Balancing National Security and Free-Speech Rights: Why Congress Should Revise the Espionage Act*, 15 COMMLAW CONSPECTUS 483, 485 (2007) ("Lawmakers and judges have characterized this language [of the Espionage Act] as ambiguous from the start."). One of the early amendments to the Espionage Act was the extension of what was known as the Section Act, which was later repealed in 1921. Sedition Act of May 16, 1918, 40 Stat. 553 (repealed Act of Mar. 3, 1921, 41 Stat. 1359).

14. Steven Aftergood, *Recipients of "Leaks" May be Prosecuted, Court Rules*, SECRECY NEWS (Aug. 10, 2006), http://blogs.fas.org/secrecy/2006/08/ (on file with the *McGeorge Law Review*) (quoting Judge T.S. Ellis, III's opinion that recipients of leaks may be prosecuted).

15. *See e.g.* Harold Edgar & Benno C. Schmidt, Jr., *The Espionage Statutes and Publication of Defense Information*, 73 COLUM. L. REV. 929, 942, 1045 (1973) ("Ambiguity pervades the Espionage Act," and there is an "overbreadth problem").

and Manning's massive Wikileaks exposé, and many critics advocate for the Act's repeal or amendment.[16]

The Espionage Act is problematic because its language encompasses more conduct than what is typically understood to constitute espionage.[17] Because of the Act's overbreadth, it is unclear what types of disclosures of national security information the government can prosecute under the Act.[18] As noted previously, the Act was primarily aimed at criminalizing traditional acts of espionage.[19] The term "espionage" generally means "the activity of using spies to collect information about what another government . . . is doing or plans to do."[20] A "spy" is "one who secretly observes and collects secret information or intelligence about what another government . . . is doing or plans to do; one who commits espionage."[21] Since the 1980s, most prosecutions under the Espionage Act are for *leaking* information that affects national security.[22] Leaking is a different problem altogether than spying in the traditional sense.[23] The fact that the government has prosecuted individuals engaged in activities outside the traditional definition of spying under the Act, even though such conduct is not clear in the statute, demonstrates the "indeterminacy about the rules of law governing defense secrets."[24]

---

16. JENNIFER K. ELSEA, CONG. RESEARCH SERV., R41404, CRIMINAL PROHIBITIONS ON THE PUBLICATION OF CLASSIFIED DEFENSE INFORMATION 16 (2013) [hereinafter CRIMINAL PROHIBITIONS REPORT] (on file with the *McGeorge Law Review*); *see e.g.* Naiman, *supra* note 11.

17. *See infra* Part III.A (discussing the methods of divulging sensitive information). "Espionage" is generally understood to mean "spying" whereby a "spy" obtains information about another government for the purposes of benefiting another. *See infra* notes 21–22. This method of espionage is much different from acts of leaking or whistleblowing, which likewise may be prosecutable under the Act. *Infra* Part III.A.

18. *See generally The Espionage Act and the Legal and Constitutional Issues Raised by WikiLeaks: Hearing Before the H. Comm. on Judiciary*, 111th Cong. 1 (2010) (prepared statement of Stephen I. Vladeck, Professor of Law, Am. Univ. Wash. Coll. of Law) [hereinafter Statement of Vladeck] (on file with the *McGeorge Law Review*) ("[T]he uncertainty surrounding this 93-year-old statute benefits no one, and leaves too many questions unanswered about who may be held liable, and under what circumstances, for what types of conduct.").

19. *See supra* note 12 and accompanying text (regarding the concerns surrounding the Act's enactment).

20. BLACK'S LAW DICTIONARY 662 (10th ed. 2014).

21. *Id.* at 1622.

22. *See e.g.,* United States v. Kiriakou, 898 F. Supp. 2d 921 (E.D.Va. 2012); Memorandum Opinion, United States v. Kim, Criminal No. 10-255 (CKK) (D.D.C. May 30, 2013); Special Findings, United States. v. Manning, Court Martial (Aug. 15, 2013) (prosecuting each of these government workers under the Espionage Act for leaking classified information).

23. A leak generally means to intentionally disclose otherwise protected information to the media or someone who is not entitled to receive it. *Compare* THE AMERICAN HERITAGE COLLEGE DICTIONARY 788 (4th ed. 2004) (defining leak as "to become publically known through a breach of secrecy" or "to disclose without authorization or official sanction") *and* THE RANDOM HOUSE WEBSTER'S COLLEGE DICTIONARY 746 (2d ed. 1997) (defining leak as "a disclosure of secret, [especially] official information by an unnamed source") *with* the general definition of espionage, "[t]he activity of using spies to collect information about what another government . . . is doing or plans to do." BLACK'S LAW DICTIONARY 662 (10th ed. 2014).

24. Edgar & Schmidt, *supra* note 15, at 936.

Additionally, advances in technology and the sophistication of the "spy" have changed the face of espionage over the last century.[25] Advances in information technology, such as the development of the Internet, the computer, and the smartphone, has allowed more "nontraditional" means of obtaining sensitive data and transmitting it to an unauthorized end user to the detriment of national security.[26] Congress has not adapted the Espionage Act as "nontraditional" motives or methods of alleged espionage have emerged,[27] thus presenting the question: *what* conduct constitutes espionage punishable under the Espionage Act?[28] Recently, the Espionage Act's provisions have come under intense public review regarding the uncertainty of how the statute applies to the press when it publishes information it obtained from a person in a forbidden manner.[29] While it may seem obvious that an initial divulger[30] could fall within the legal framework of the Espionage Act,[31] there is still a great deal of uncertainty about when the Espionage Act applies, if it applies at all, to that

25. *See* KATHERINE L. HERBIG, DEFENSE PERSONNEL SECURITY RESEARCH CENTER, CHANGES IN ESPIONAGE BY AMERICANS: 1947–2007 66, 70 (2008) [hereinafter CHANGES IN ESPIONAGE] (on file with the *McGeorge Law Review*) (explaining "[w]hat has changed is the ubiquity of spies' reliance on electronic files for copying, storing, transmitting, and hiding" and that "the laptop computer, the thumb drive storage device, and the Internet have only made espionage quicker and easier"). In addition, the author points to eleven individuals who conducted espionage activities between 2000 and 2007, most of which "made use of computer technology to retrieve, store, and transfer information," with "many of them [making] use of the Internet to make or maintain contact with customers." *Id.*

26. *See id*. and accompanying text.

27. *See* Aftergood, *supra* note 14 (quoting Judge T.S. Ellis, III's opinion that "provisions of the Espionage Act 'have remained largely unchanged since the administration of William Howard Taft'"). *See also* CHANGES IN ESPIONAGE, *supra* note 25, at 32, 70 (showing changes in motives of spies over time). Some historical motives for espionage include money, divided loyalties, disgruntlement, ingratiation, coercion, thrills, and recognition or ego. *Id*. If leaking and whistleblowing are to be considered acts of espionage, then these may present additional changes in motive, something the Espionage Act fails to take into account. *See infra* Part III.A (discussing methods of divulging sensitive information).

28. This question also includes: *who* can be charged with espionage under the statute? *See infra* note 30 and accompanying text.

29. CRIMINAL PROHIBITIONS REPORT, *supra* note 16; s*ee e.g.* Caplan, *supra* note 8 (discussing issues on the publication of sensitive information).

30. The term "initial divulger" is intended to mean the first individual who discloses information in a way that is prohibited by the Espionage Act (which is typically a government official who has access to sensitive or classified national security information). It is used as a blanket term as opposed to "leaker" or "whistleblower" or "spy," which are distinct from one another. *See infra* Part III.A (discussing who and how information is divulged). While the Espionage Act presumably covers more than just the initial divulger, including third-party recipients of sensitive information, this Comment focuses primarily on the initial divulger and whether his actions fall within the meaning of the language of Espionage Act. *See also* Statement of Vladeck, *supra* note 18, at 2 ("[T]he Espionage Act does not focus solely on the initial party who wrongfully discloses national defense information, but applies, in its terms, to *anyone* who knowingly disseminates, distributes, or even *retains* national defense information without immediately returning the material to the government officer authorized to possess it. In other words, the text of the Act draws no distinction between the leaker, the recipient of the leak, or the 100th person to redistribute . . . the national defense information that, by this point, is already in the public domain.").

31. *See Viewpoints: The Bradley Manning Verdict*, BBC NEWS (July 30, 2013, 5:40 PM), http://www.bbc.com/news/world-us-canada-23511145 (on file with the *McGeorge Law Review*) (with Nathan Sales noting that "Manning's conviction is a fairly routine application of well-settled legal principles.").

initial divulger whose actions and motivations are at the epicenter of heated public debate.[32]

This Comment proposes that the Espionage Act needs revision as applied to the initial divulger of protected information in order to remove ambiguity and allow a more consistent and appropriate application of the law. Moreover, the Espionage Act should provide certainty as to what conduct constitutes espionage or what conduct is punishable under its provisions, as well as potentially deter and prevent leaks.[33] Part II provides a brief history of the Espionage Act and a breakdown of its most notable sections. Part III looks specifically at what the Espionage Act says in its most troublesome sections by analyzing the statutory language, legislative history, and appellate and pending cases in order to illustrate its ambiguity, overly broad terminology, and confusing provisions. Part IV proposes changes to the Act that will result in a clearer and more consistent application of the law thus enabling the government to effectively prosecute legitimate acts of espionage and detrimental leaks by an initial divulger of protected information.

II. THE ESPIONAGE ACT

> *"If there should be disloyalty, it will be dealt with with a firm hand of stern repression."*
>
> *—President Woodrow Wilson*[34]

A. A Brief History of the Espionage Act

In April 1917, the United States marched into the heat of battle in World War I, and had a legitimate concern "to try to stop the real threat of subversion, sabotage, and malicious interference with the war effort, including the controversial reinstatement of the draft."[35] But Congress hotly debated the scope

---

32. *Compare* John Cassidy, *Why Edward Snowden is a Hero*, THE NEW YORKER (June 10, 2013), http://www.newyorker.com/online/blogs/johncassidy/2013/06/why-edward-snowden-is-a-hero.html (on file with the *McGeorge Law Review*) (explaining why Snowden should be characterized as a hero while acknowledging some disagree), *with* Jeffrey Toobin, *Why Edward Snowden is No Hero*, THE NEW YORKER (June 10, 2013), http://www.newyorker.com/online/ blogs/comment/2013/06/edward-snowden-nsa-leaker-is-no-hero.html (on file with the *McGeorge Law Review*) (explaining why Snowden is not a hero nor a whistleblower, characterizing him as " a grandiose narcissist who deserves to be in prison.").

33. It is clear that the United States Government wants to prosecute leaks because they do not want to give the indication that such disclosure would be acceptable or unpunishable. *See generally* Caplan, *supra* note 8 (explaining that "the government seems more concerned about maintaining control than doing justice"). This lends itself to the prevention aspect by not allowing "copycats" or an increase in potentially compromising leaks.

34. MESSAGE FROM PRESIDENT WILSON TO CONGRESS, Apr. 2, 1917, in 55 CONG. REC. 104 (1917) [*hereinafter* MESSAGE FROM PRESIDENT WILSON].

35. Rozenshtein, *supra* note 12 (quoting David Greenberg); *see* Kennedy, *supra* note 12, at 24 ("During the period of American neutrality, German agents had committed acts of sabotage and tried to foment labor troubles in East Coast ports and factories, in order to disrupt the delivery of war material to the Allies. In 1915

of the Espionage Act, which was originally much broader than the version actually passed.[36] Indeed, some critics point to President Wilson's ulterior motive of establishing "broad controls" that "would have given the President full power to restrict the divulgence of government secrets, public access to defense places, and public discussion and reporting of matters relating to the war."[37] However, Congress declined to pass proposed provisions such as censoring the press and filtering the mail, and eventually agreed upon the 1917 version of the Espionage Act.[38]

President Wilson, in asking Congress to declare war, remarked that "[f]rom the very outset of the present war it has filled our unsuspecting communities and even our offices of government with spies and set criminal intrigues everywhere afoot against our national unity of counsel, our peace within and without, our industries and our commerce."[39] The President's real concern was spies within the government having access to national defense information and communicating that protected information to wartime enemies.[40] But even if the Espionage Act was necessary to address perceived concerns, it proved difficult to apply from its onset.[41] Eager prosecutors punished many anti-war dissidents under the Act's expansive provisions.[42] Prosecutors use the Act as a general sanction to prosecute any perceived disloyal conduct, and not necessarily for wrongful disclosures of national defense information.[43] The legislative history

---

Wilson had expelled the German military and naval attachés from the country for their connection with those intrigues. . . . [President Wilson] had [also] gone on in late 1915 and 1916 to launch a broad attack against so-called hyphenated Americans.").

36. Epstein, *supra* note 13, at 486.

37. Edgar & Schmidt, *supra* note 15, at 946.

38. Rozenshtein, *supra* note 12.

39. MESSAGE FROM PRESIDENT WILSON, *supra* note 34, at 104.

40. *Stephen Vladeck on Espionage Act* (C-SPAN live broadcast Mar. 10, 2012), *available at* http://www.c-span.org/video/?304857-5/stephen-vladeck-espionage-act (on file with the *McGeorge Law Review*).

41. Epstein, *supra* note 13, at 485; Caitlin Dewey, *Manning was Charged Under the Espionage Act. It Doesn't Have a Proud History*, WASH. POST (July 31, 2013), www.washingtonpost.com/blogs/the-switch/wp/2013/07/31/manning-was-charged-under-the -espionage-act-it-doesnt-have-a-proud-history/ (on file with the *McGeorge Law Review*).

42. Dewey, *supra* note 41; *see* David Greenberg, *The Hidden History of the Espionage Act*, SLATE (Dec. 27, 2010), www.slate.com/articles/news_and_politics/history_lesson?2010/12/the_hidden_history_of_the_espionage_act.1.html (on file with the *McGeorge Law Review*) (noting that "[the Espionage Act], even in its softer version, left far too much room for aggressive prosecutors and overzealous patriots to interpret it as they wished."). *See e.g.,* Schenck v. United States, 249 U.S. 47-48, 52-53 53 (1919) (upholding Schenck's conviction under the Espionage Act for distribution of leaflets criticizing the war, and ultimately holding that the Espionage Act did not violate his free speech rights).

43. Greenberg, *supra* note 42. While the prosecutions of anti-war protesters were excessive, it is uncertain how many prosecutions were for leaks or disclosures of defense information, if any. *See id.* ("U.S. attorneys in Thomas Gregory's Justice Department prosecuted socialists, pacifists, and German-Americans on flimsy grounds. Many people were arrested for crimes of mere speech. . . . Of 1,500 arrests under the law, only 10 involved actual sabotage. To the dismay of progressives, moreover, not even the Supreme Court stopped the prosecutions. In March 1919, the liberal icon Oliver Wendell Holmes, coining his famous 'clear and present danger' standard, led the court in upholding three dubious Espionage Act verdicts, including the conviction of Debs."). *See e.g.* Debs v. United States, 249 U.S. 211–212 (1919); *Schenck*, 249 U.S. at 48-49 (convicted under

and contentious discussions that surrounded the law's enactment indicate that the public frowned upon overzealous prosecutions under the Act's provisions.[44] These prosecutions did not seem to fit the type of conduct the legislature meant to criminalize—traditional acts of spying and sabotage.[45] Congress has amended the Espionage Act several times,[46] but the most pertinent sections of the Act under which most past and present prosecutions occur remain largely unchanged from the 1917 version.[47]

B. The Core Sections of the Espionage Act

The Espionage Act contains seven sections, but most uncertainty stems from sections 793 and 794, which each contain various subsections.[48] Section 793 is probably the most confusing section because it encompasses multiple circumstances for which one can be prosecuted under the Act.[49]

1. Section 793

Generally, this section criminalizes disclosures of information "respecting" or "relating to" the national defense.[50]

Subsections 793(a) and (b) are often lumped together in explaining their applicability.[51] These subsections prohibit "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" by entering a military installation, obtaining information concerning military-related activities, or otherwise gathering information "connected with the national defense."[52] Thus, based on the statutory language, the initial divulger must have the requisite scienter, "intent or reason to believe" that the information could be used to injure the U.S.[53] This scienter must exist when there is any revelation of

---

the Espionage Act for actions that the government perceived as detrimental to the war effort).

44. Greenberg, *supra* note 42.

45. *Id.*

46. *See supra* note 13 (regarding the Sedition Act amendment and repeal).

47. Epstein, *supra* note 13, at 493; Edgar & Schmidt, *supra* note 15, at 939.

48. 18 U.S.C. §§ 792–798 (2012); Edgar & Schmidt, *supra* note 15, at 937–38.

49. *See infra* Part II.B.1 (discussing the confusion surrounding this provision).

50. 18 U.S.C. § 793.

51. Edgar & Schmidt, *supra* note 15, at 967–68; GEOFFREY R. STONE, FIRST AMENDMENT CENTER, GOVERNMENT SECRECY V. FREEDOM OF THE PRESS 36 (2006) [hereinafter GOVERNMENT SECRECY] (on file with the *McGeorge Law Review*).

52. 18 U.S.C. § 793(a)–(b).

53. The requisite injury includes the entire phrase "injury to the United States, or advantage of any foreign nation," although it may be truncated at times throughout the Comment for brevity.

"information respecting the national defense."[54] In short, these subsections "prohibit the collection of" information relating to the national defense.[55]

Subsection 793(c) extends to individuals beyond the initial divulger, in that it forbids anyone who "obtains or agrees or attempts to receive" documents and other tangible items "connected with the national defense, knowing or having reason to believe . . . that [such information] has or will be obtained" by a person who has violated a provision of the Act.[56] In this provision, there is no facial intent requirement as in 793(a) or (b); the recipient or potential recipient need only have "know[ledge]" or "reason to believe" that the initial divulger obtained the information in a manner inconsistent with other sections of the Act.[57] Thus, this subsection "prohibits the receipt of" information connected with the national defense, including attempts at receipt of such information, if the recipient knows or should know that the initial divulger "violated some other provision of the Espionage Act."[58]

Subsections 793(d) and (e) apply specifically, and most sweepingly, to the initial divulger (and potentially to third party publishers).[59] Subsections 793(d) and (e) prohibit a person "lawfully having possession of" or a person having "unauthorized possession of," respectively, tangible items or information "relating to the national defense" which the "possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, [from] willfully communicat[ing], deliver[ing], transmit[ing], or cause[ing] to be communicated [such information] . . . to any person not entitled to receive it."[60] Under these subsections, a divulger need only "willfully" communicate the information rather than communicate "with intent or reason to believe" as in other sections.[61] Thus, "willful" disclosure may be easier for prosecutors to demonstrate since it does not require a showing of specific intent.[62]

The government charges and ultimately prosecutes or pleads out many leakers under section 793(d) or 793(e),[63] likely because the subsections are extremely broad and do not require any specific criminal intent that the

54. 18 U.S.C. § 793(a)–(b).

55. GOVERNMENT SECRECY, *supra* note 51, at 36.

56. 18 U.S.C. § 793(c).

57. *Id.* § 793(a)–(c); Edgar & Schmidt, *supra* note 15, at 938.

58. GOVERNMENT SECRECY, *supra* note 51, at 36–37.

59. Edgar & Schmidt, *supra* note 15, at 938.

60. 18 U.S.C. § 793(d)–(e).

61. GOVERNMENT SECRECY, *supra* note 51, at 37, 39 (intent as in section 793(a)–(b) and 794(a)–(b)).

62. *Id.* at 37.

63. *See e.g.* United States v. Morison, 844 F.2d 1057, 1063 (4th Cir.1988) (charged and prosecuted under sections 793(d), (e)); United States v. Rosen, 445 F. Supp. 2d 602, 607, 610 (E.D.Va. 2006) (charged and prosecuted under sections 793(d), (e), among other charges); Special Findings, United States v. Manning, Court Martial (Aug. 15, 2013) (charged and prosecuted under section 793(e), among other charges); Memorandum Opinion, United States v. Kim, Criminal No. 10-255 (CKK) (D.D.C. May 30, 2013) (charged and pending prosecution under section 793(d)); Criminal Complaint, United States v. Snowden, No. 1:13 CR 265 (E.D.Va. June 14, 2013) (charged under section 793(d), among other charges).

information will be used to injure the United States.[64] Similarly, the media could violate section 793(e) by publishing leaked information, even in absence of actual intent, if they "willfully" communicated the information.[65]

2. Section 794

Generally, this section covers the traditional understanding of a "spy," and addresses providing information to aid a foreign government.[66]

Subsection 794(a) criminalizes the communication or transmission of any tangible item or "information relating to the national defense" to a foreign government or citizen thereof with "intent or reason to believe that it is to be used to the injury of the United States or to the advantage of a foreign nation."[67] It carries with it a possible death sentence.[68] Like 793(a) and (b), prosecutors must prove intent under this section.[69]

Subsection 794(b) provides that an individual "in time of war, with the intent that the same shall be communicated to the enemy . . . communicates or attempts to elicit any information" regarding military operations "which might be useful to the enemy, shall be punished by death or by imprisonment."[70] This provision is narrower than subsection 793(a) because it applies only during wartime and only to the communication of information to an *enemy*, as opposed to *any* foreign nation.[71]

III. THE TROUBLE WITH PROSECUTING ESPIONAGE UNDER THE ESPIONAGE ACT AND THE NEED FOR CHANGE

> *"Technically, we whistleblowers broke the law, but we felt, as many have felt before, that the obligation to our consciences and basic human rights is stronger than our obligation to obey the law."*
>
> *—Shamai Leibowitz*[72]

64. *See* GOVERNMENT SECRECY, *supra* note 51, at 37 ("Section 793(e) therefore appears to have a far more relaxed intent requirement than §§ 793(a) and 793(b). The provision does not require specific intent so long as the communication or retention of classified information is willful.").

65. *Id.*

66. 18 U.S.C. § 794.

67. *Id.* § 794(a).

68. *Id.*.

69. *Id.* §§ 793(a)-(b), 794(a).

70. *Id.* § 794(b). Section 794 also contains subsections (c)–(d) which cover inchoate liability and sentencing, respectively. *Id.* §794(c)–(d).

71. Edgar & Schmidt, *supra* note 15, at 945.

72. Shamai Leibowitz, *Blowback from the White House's Vindictive War on Whistleblowers*, The GUARDIAN (July 5, 2013, 8:30 AM), http://www.theguardian.com/commentisfree/2013/jul/05/blowback-white-house-whistleblowers (on file with the *McGeorge Law Review*). Leibowitz was formerly a contract linguist for the FBI who leaked classified information to an online blogger. *Id.* In December 2009, he was charged under section 798(a)(3) of the Espionage Act for willful disclosure of classified information, and ultimately took a

Nearly forty years ago, scholars pointed out that "[a]mbiguity pervades the Espionage Act."[73] Yet, despite various proposals to amend the Act, it remains substantially similar to its 1917 form.[74] In addition, the evolved methods of divulging information, including leaks and whistleblowing, need consideration in prosecuting an individual under the Espionage Act.[75]

A. Methods of Divulging Information by an Individual Working for or on Behalf of the Government

The Espionage Act is problematic because it lumps together different types of conduct, without clear differentiation, for which a person can be prosecuted.[76] This type of conduct goes beyond classic espionage, but the government does not seem interested in distinguishing "leaking" from "espionage."[77] Although not express, modernly, there appear to be three primary categorizations of conduct that could ultimately lead to prosecution for the initial divulger under the Espionage Act: (1) improper whistleblowing; (2) impermissible leaking; and (3) spying.[78] While these categorizations may just be labels, the characterizations are important because the motivations, methods of disclosure, and target recipients differ.[79]

1. Whistleblowing

A whistleblower is "[a]n employee who reports employer wrongdoing to a governmental or law-enforcement agency."[80] A whistleblower's primary motive

---

plea deal for 20 months in prison. *Id.*; Criminal Complaint, United States v. Leibowitz, No. AW09 CR 0632 (D. Md. Dec. 4, 2009).

73. Edgar & Schmidt, *supra* note 15, at 942.

74. *See e.g.* Steven Aftergood, *Senate Bill Would Make Leaks a Felony*, SECRECY NEWS (Feb. 17, 2011), http://blogs.fas.org/secrecy/2011/02/cardin_leaks (on file with the *McGeorge Law Review*) (discussing a 2011 proposal to amend the Espionage Act to criminalize disclosure of any classified information, as well as the SHIELD act, a proposal to criminalize unauthorized disclosure of information related to human intelligence activities); The Espionage Act of 1917, 40 Stat. 217–20.

75. *See supra* Part II.A (discussing the types of conduct that constitute espionage).

76. *See e.g.* 18 U.S.C. §§ 793–794; *see also supra* Part II.B (discussing these core sections of the Espionage Act).

77. *See supra* Part II.B (discussing the basic provisions of the Espionage Act); *see also* Caplan *supra* note 8 (noting "[t]he executive branch . . . has little incentive to give up any tool of law useful in deterring terrorism.").

78. *See generally* Statement of Vladeck, *supra* note 18, at 2 ("[T]he government has traditionally been forced to shoehorn into the Espionage Act three distinct classes of cases that raise three distinct sets of issues: classic espionage; leaking; and the retention or redistribution of national defense information by private citizens.") While "whistleblowing" is a form of "leaking" if the whistleblower improperly discloses sensitive information, this Comment distinguishes this conduct because of the subjective intent of the whistleblower. *See infra* Part III.A.2 (distinguishing improper whistleblowing and unauthorized leaking).

79. *See* Statement of Vladeck, *supra* note 18, at 2 (discussing the Espionage Act's deficiency in dealing with disclosure of information in non-espionage cases, forcing the government to categorize the issues).

80. BLACK'S LAW DICTIONARY 1831 (10th ed. 2014).

is to speak out against government misconduct.[81] Comparatively, the Whistleblower Protection Act of 1989[82] defines a whistleblower as someone who "reasonably believes [government conduct] evidences [a] violation of [a] law, rule, or regulation or gross mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety."[83] However, a whistleblower must be able to prove "illegal or improper government activities" as opposed to self-perceived assertions of immoral or illegal conduct.[84] The whistleblower must follow a set of internal procedures to properly blow the whistle on such misconduct.[85] When a perceived whistleblower improperly discloses protected information in pursuit of blowing the whistle on government misconduct, the inquiry becomes, to what extent should the Espionage Act apply? The whistleblower's subjective intent is to do "a good thing" or merely inform the American public of government wrongdoing, not to harm to the United States or otherwise help a foreign government.[86] Although whistleblower statutes do not cover all government employees and the procedures can result in a lengthy reporting process, potential employer retaliation, or other undesirable consequences,[87] Congress enacted such laws to protect whistleblowers by

---

81. L. PAIGE WHITAKER CONG. RESEARCH SERV., RL33918, THE WHISTLEBLOWER PROTECTION ACT: AN OVERVIEW 1 (Mar. 12, 2007) [hereinafter CRS REPORT FOR CONGRESS] (on file with the *McGeorge Law Review*).

82. 5 U.S.C. § 1221 (2012).

83. *Id.* § 2302(b)(8)(A)(i)–(ii). However, the employee must be covered under the Act in order to enjoy its categorizations and protections. *See infra* note 88 and accompanying text (explaining the provisions of the Act).

84. CRS REPORT FOR CONGRESS, *supra* note 81, at 1.

85. *See e.g., id.* (regarding the Whistleblower Protection Act of 1989,

> [g]enerally, whistleblower protections may be raised within four forums or proceedings: (1) employee appeals to Merit Systems Protection Board of an agency's adverse action against an employee, known as 'Chapter 77' appeals; (2) actions instituted by the Office of Special Counsel; (3) individually maintained rights of action before the Merit Systems Protection Board (known as an individual right of action, or IRA); and (4) grievances brought by the employee under negotiated grievance procedures.).

There are several other federal statutes and directives that protect whistleblowers, but they are not comprehensive, and leave several government workers unaccounted for. *See infra* note 88 and accompanying text (discussing the different statutes and directives that cover whistleblowing and their shortcomings).

86. *See e.g.* Andrea Peterson, *Snowden: I Raised NSA Concerns Internally Over 10 Times Before Going Rogue*, WASH. POST (Mar. 7, 2014, 10:58 AM), http://www.washingtonpost.com/blogs/the-switch/wp/2014/03/07/snowden-i-raised-nsa-concerns-internally-over-10-times-before-going-rogue/?print=1 (on file with the *McGeorge Law Review*) ("Edward Snowden said that he repeatedly tried to go through official channels to raise concerns about government snooping programs."), *but see* Agence France-Presse, *Snowden Didn't Raise Concerns Internally: NSA*, BUS. INSIDER (Sept. 13, 2014, 6:21 AM), http://www.businessinsider.com/afp-snowden-didnt-raise-concerns-internally-nsa-2014-9 (on file with the *McGeorge Law Review*) (explaining that the NSA's internal investigation found nothing to support Snowden's assertion that he raised concerns about the NSA's surveillance programs to agency officials).

87. *See e.g.* Peterson, *supra* note 86 (quoting Edward Snowden regarding his decision to expose classified information through the media)

> Yes. I had reported these clearly problematic programs to more than ten distinct officials, none of whom took any action to address them. As an employee of a private company rather than a direct employee of the US government, I was not protected by the US

allowing them to bring forth grievances in a manner that does not violate the Espionage Act.[88] While the public might use the term "whistleblower" to mean someone that generally reveals government misconduct, this perception does not necessarily bring that individual within the protection of the whistleblower statutes.[89] Even if the information exposes illegal government conduct, the divulger is not a legal whistleblower if he or she does not follow the proper channels of reporting.[90] If an individual discloses protected information to the media, it would constitute leaking notwithstanding the individual's well-intentioned disclosure.[91]

2. Leaking

Leaking, on the other hand, has no legal definition; it largely remains an informal term. [92] However, a typical leak is an intentional disclosure of otherwise protected information to the media or someone who is not entitled to receive it.[93] Section 793 of the Espionage Act broadly covers this type of conduct, albeit confusingly.[94] This is because the motive or intent behind such leaks are difficult to ascertain, and the scienter element differs depending on which subsection of the Espionage Act such conduct falls into.[95] Leaks generally fall into one of three

---

> whistleblower laws, and I would not have been protected from retaliation and legal sanction for revealing classified information about lawbreaking in accordance with the recommended process.

Id.

88. 5 U.S.C. §§ 1201–1222 (2012). This law is known as the Whistleblower Protection Act, but does not apply to members of the intelligence community or enable any whistleblower defense in a criminal case. *Id.*; Intelligence Community Whistleblower Protection Act of 1998, Pub. L. No. 105–272, §§ 702–703, 112 Stat. 2396 24–17 (allowing members of the intelligence community to report "urgent concerns," including concerns referencing classified information, through the Inspector General, but does not provide retaliation protections or allow a whistleblower defense in a criminal case); Inspector General Act of 1978, 5 U.S.C. App. § 7 (providing a mechanism by which Department of Defense employees can file a complaint without reprisal or revelation of identity); Protecting Whistleblowers with Access to Public Information, PRESIDENTIAL POLICY DIRECTIVE 19 (Oct. 10, 2012) (on file with the *McGeorge Law* Review) (providing protections to intelligence agency members whistleblowers with access to classified information, but leaving several gaps, such as the inclusion of government contractors within its directives); 10 U.S.C. § 1034 (2012) (protecting communications by military members to Congress and the Inspector General and prohibiting retaliation against a military member).

89. *See e.g.* Erik Wemple, *Edward Snowden: 'Leaker,' 'Source,' or 'Whistleblower*,' WASH. POST (June 10, 2013, 9:03AM), http://www.washingtonpost.com/blogs/erik-wemple/wp/2013/06/10/edward-snowden-leaker-source-or-whistleblower (on file with the *McGeorge Law Review*) (quoting Glenn Greenwald of *The Guardian*) ("I don't think 'whistleblower' requires revelation of illegal conduct."); *See also* Peterson, *supra* note 86 (explaining that Edward Snowden's employment status would not allow him protection under US whistleblower laws).

90. CRS REPORT FOR CONGRESS, *supra* note 81, at 1.

91. *See supra* Part III.A. (noting that whistleblowing is a type of leaking, but is distinguishable for purposes of the Espionage Act as to the extent subjective intent applies).

92. *See generally* Wemple, *supra* note 89 (discussing the trouble with defining and construing the terms used).

93. *See supra* note 23 and accompanying text (generally defining "leaking" and "spying").

94. *See infra* Part III.B. (regarding the confusing language of the Espionage Act).

95. Steven Aftergood, *Not all Leaks of Classified Information Violate the Law,* SECRECY NEWS (June 13,

categories: (1) unauthorized leaks; (2) authorized leaks; and (3) third party leaks.[96]

Unauthorized leaks can easily fall within the broad language of Sections 793(d) and (e) of the Espionage Act—that is, the willful communication or transmission of "information relating to the national defense" to persons "not entitled to receive it."[97] Essentially, the Act prohibits the disclosure of such information without proper authorization because the information is supposed to remain protected.[98]

Authorized leaks, or leaks that are not considered criminal, are typically disclosures of sensitive information that occur with permission or happen on a routine basis.[99] These types of leaks largely go unpunished, unnoticed, and unacknowledged as leaks at all, and are often difficult to distinguish from unauthorized leaks.[100]

Third party leaks typically concern the publication of sensitive information by a third party who received the information from a primary divulger (that is, the third party did not have first-hand knowledge of the information).[101] The third party recipient is generally a media or news source who publishes the information for public distribution.[102] While there has been at least one prosecution of a non-news media third party recipient who subsequently disclosed the protected information,[103] typically third party leaks occur through

---

2012), http://fas.org/sgp/news/secrecy/2012/06/061312.html (on file with the *McGeorge Law Review*) [hereinafter Aftergood, *Not all Leaks*].; *see supra* Part II.B (describing the subsections of the Espionage Act).

96. *See generally* Aftergood, *Not all Leaks*, *supra* note 95 (explaining that "there is no law that categorically prohibits the release of classified information."); *see also* Steven Aftergood, *Dept of Defense to Report on "Authorized Leaks,"* SECRECY NEWS (Oct. 15, 2013), http://fas.org/sgp/news/secrecy/2013/10/101513.html [hereinafter Aftergood, *Dept of Defense*] (regarding different characteristics for which leaks can be criminal).

97. 18 U.S.C. § 793(d)–(e) (2012).

98. *See generally* Steven Aftergood, *What is an Unauthorized Disclosure,* SECRECY NEWS (Aug. 1, 2012), http://blogs.fas.org/secrecy/2012/08/unauthorized_disclosure (on file with the *McGeorge Law Review*) [hereinafter Aftergood, *What is an Unauthorized Disclosure*] (noting "[t]hough the answer may seem obvious, it is actually subject to conflicting interpretations.").

99. *See* Aftergood, *Some Unauthorized Disclosures*, *supra* note 11 (noting that "classified information is frequently disclosed at the interface between national security agencies and the news media . . . [I]t is how the system normally functions."). "[T]he peculiar reality is that certain officials routinely take it upon themselves to discuss classified information with unauthorized persons." *Id.*

100. *See* Aftergood, *Not all Leaks*, *supra* note 95 ("Even when 'national defense' information that is clearly covered by the [Espionage] Act is disclosed to an unauthorized person, it does not necessarily follow that a crime has been committed."). The "requisite criminal intent" must also be present in order to be prosecuted under the Espionage Act. *Id. See also* Aftergood, *What is an Unauthorized Disclosure*, *supra* note 98 ("A new Department of Defense directive requires the Pentagon to notify Congress whenever a DoD official discloses classified intelligence to a reporter on an authorized basis."). *See e.g.,* Naiman, *supra* note 11 (explaining "[The Espionage Act] allows selective prosecution of whistle-blowers on an extreme charge.").

101. CRIMINAL PROHIBITIONS REPORT, *supra* note 16, at 16.

102. *Id.*

103. United States v. Rosen, 445 F.Supp.2d 602, 643 (E.D.Va. 2006) (involving unauthorized disclosure by a government employee to others who worked for or with the government who subsequently published the information); *see infra* notes 134–138 and accompanying text (discussing *United States v. Rosen*).

press publication.[104] However, it remains unclear whether the federal government can prosecute a media recipient under the Espionage Act for publication of such defense information, specifically under subsection 793(e).[105]

3. Spying

A "spy" is "one who secretly observes and collects secret information or intelligence about what another government . . . is doing or plans to do; one who commits espionage."[106] Traditionally, spying involved the clandestine collection of information from one government and transmission of information to another government or adversary who has employed the spy.[107] Section 794 of the Espionage Act broadly covers this type of conduct.[108] Generally, most acts by individuals who are charged under section 794 are obvious violations and ultimately the spy enters a plea agreement.[109] With virtually no case law on the matter, the application of section 794 remains unclear, as do the applications of other sections of the Act.[110]

B. The Confusing Language

Much of the ambiguity in the Espionage Act stems from the language of the statute itself.[111] Two distinct elements of the statutory language pose challenges to the interpretation and understanding of the Espionage Act: (1) the type of information that the Act prohibits from disclosure, and (2) the requisite intent.[112]

---

104. CRIMINAL PROHIBITIONS REPORT, *supra* note 16, at 16.

105. The issue of whether or not third party publication is punishable under the Espionage Act is outside the scope of this Comment, but an important consideration in amending the Espionage Act. For more information, *see* CRIMINAL PROHIBITIONS REPORT, *supra* note 16, and GOVERNMENT SECRECY, *supra* note 51.

106. BLACK'S LAW DICTIONARY 1622 (10th ed. 2014).

107. *See* FBI COUNTERINTELLIGENCE NATIONAL STRATEGY, A BLUEPRINT FOR PROTECTING U.S. SECRETS, FED. BUREAU OF INVESTIGATION (2011), *available at* http://www.fbi.gov/news/stories/2011/november/counterintelligence_110411 (on file with the *McGeorge Law Review*) (describing how spying is no longer just "passing U.S. secrets to foreign governments, either to fatten [spies'] own wallets or to advance their ideological agendas.").

108. 18 U.S.C. § 794 (2012).

109. *See e.g. Famous Cases & Criminals: Aldrich Hazen Ames*, FED. BUREAU OF INVESTIGATION, http://www.fbi.gov/about-us/history/famous-cases/aldrich-hazen-ames (last visited Nov. 16, 2014) (on file with the *McGeorge Law Review*) (regarding former CIA agent Aldrich Ames, charged under subsection 794(d) of the Espionage Act for spying for Russia and who pled guilty for a sentence of life in prison); Plea Agreement, United States v. Hanssen, Cr. No. 01-188-A (E.D.Va. July 6, 2001) (charging former FBI agent Robert Hanssen under subsection 794(a) and (c) of the Espionage Act for spying for Soviet and Russian intelligence services, who pled guilty in exchange for life in prison).

110. *See infra* section III.B (regarding the confusing language in the core sections of the Espionage Act).

111. Edgar & Schmidt, *supra* note 15, at 938–39.

112. *See id.* (stating that

> "[t]he major questions concerning the espionage statutes are: (1) what type of revelation or communication is a necessary element of the particular offense. . . . (2) what state of mind with respect to the consequences for United States' interests is made a material element of the

The following sections analyze the problems with modern "espionage" by delving into the statutory language, the legislative history, and the applicable case law for each of the contentious elements of the Act.[113]

1. Information Respecting, Connected to, or Relating to the National Defense

Under subsections 793(a)–(e) and 794(a)–(b), the information that the divulger disclosed must be one of the multiple items specifically listed or information relating to, connected to, or respecting the national defense.[114] Thus, these sections purport to make disclosure of any information respecting the national defense criminal.[115] Broadly construed, this means that anything rationally or conceivably tied to national security could be subject to charges under the Act.[116]

The legislative history notes that some Congress Members cautioned against the broad and sweeping language, but such language went unchanged.[117] The acceptance of such an expansive phrase was predominately based on a lack of alternative terminology or limiting specificity; the legislature intended to ensure that the statute adequately encompassed all information the government believed to be sensitive.[118] The 64th and 65th Congresses did not consider the term "classified" because the United States had not yet adopted a formal system of classification.[119] Classified information is information identified by a designated classification authority as requiring "protection in the interests of preserving

---

different offenses. . . . and (3) what information is subjected to statutory restraints under the various standards ranging from 'information related to the national defense' to 'classified communications intelligence'").

113. *See infra* Part III.B.1–2 (discussing the confusion with the Espionage Act).

114. 18 U.S.C. §§ 793(a)–(e), 794(a)–(b) (2012) (each of the subsections say either "respecting," "connected to," or "relating to the national defense").

115. *Id.*

116. *See* Edgar & Schmidt, *supra* note 15, at 969 (noting "[t]he principal problem in construing ['national defense'] is to find its limits in an era when every facet of civilian life may have an important bearing on the nation's military capabilities.").

117. *See e.g.,* 54 CONG. REC. 3485 (1917) (Senator Cummins asking "What is the national defense? Those words are not defined; they are in no ways qualified or restricted. . . . I should think that it would include everything from the mines and the forests which ultimately passes into the structures or the arms that are used in war, no matter whether they are used immediately in battle, or whether they are used in general connection with the Army or Navy.").

118. *See e.g.,* 54 CONG. REC. 3601 (1917) (Senator Overman stating "[i]t would be impossible to specify these places. . . . we made [the term 'national defense'] general to protect everything connected with the national defense.").

119. The United States classification system formally came into existence in 1940, and involves "identifying . . . information which requires protection in the interests of preserving national security." N. Cathy Maus, Office of Declassification, *History of Classification and Declassification*, FED'N OF AM. SCIENTISTS (July, 22, 1996) *available at* http://www.fas.org/irp/doddir/doe/history.htm (on file with the *McGeorge Law Review*).

national security."[120] The Espionage Act does not define the term "national defense," nor is the meaning of the term obvious on its face.[121] Modernly, a substantial amount of sensitive information relating to the national defense is classified.[122] With the ambiguous term "national defense" in the statute and little precedent, judges are left to interpret what this term encompasses.[123]

In *Gorin v. United States*, the United States Supreme Court interpreted the meaning of the term "related to the national defense."[124] In 1940, Gorin, a citizen of the U.S.S.R., paid Salich, a United States Naval Intelligence Officer, for counterintelligence reports regarding Japanese movement and other activities.[125] The government charged both men under sections 793(b) and 794(a) of the Espionage Act.[126] The defendants asserted that the Espionage Act was "unconstitutional as violative of due process because of indefiniteness."[127] They argued that the statute was unconstitutionally vague because virtually everything can relate to the national defense.[128] The court rejected the defense, finding that the scienter requirement sufficiently limits the phrase.[129] In defining the term, the court stated, "[n]ational defense. . .'is a generic concept of broad connotations, referring to the military and naval establishments and the related activities of national preparedness.'"[130] Without much discussion, the court held the counterintelligence reports at issue could be related to the national defense and sent the question to the jury.[131] The jury found the reports were connected with military activity, and thus, related to the national defense.[132]

In *United States v. Rosen,* the court further interpreted the phrase "relating to the national defense".[133] There, prosecutors charged Steven Rosen, the former director of foreign policy issues of the American Israel Public Affairs Committee (AIPAC), along with Keith Weissman, the former senior Middle East analyst for AIPAC, under subsections 793(e) and (g) of the Espionage Act for disclosing classified intelligence and foreign policy reports on the Middle East.[134] Lawrence

120. *Id.*

121. *See* 18 U.S.C. §§ 792–798 (2012) (showing that the term "national defense" is not explicitly defined).

122. *See generally* Maus, *supra* note 119 and accompanying text (explaining process of classification and how it relates to national defense).

123. Edgar & Schmidt, *supra* note 15, at 974.

124. *Id.*; Gorin v. United States, 312 U.S. 19, 25 (1941).

125. *Gorin*, 312 U.S. at 22–23.

126. *Id.* at 21–22 (formerly sections 1(b) and 2(a) under the original Espionage Act of 1917, 40 Stat. 217–220).

127. *Id*. at 23.

128. *See id.* at 24 ("Petitioners argue that the statute should not be construed so as to leave to a jury to determine whether an innocuous report on a crop yield is "connected" with the national defense.").

129. *Id.* at 27–28; *see infra* Part III.B.2 (discussing the scienter element under those subsections).

130. *Gorin,* 312 U.S. at 28.

131. *Id*. at 31–32; Edgar & Schmidt, *supra* note 15, at 975–76.

132. *Gorin*, 312 U.S. at 31–32.

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

134. Epstein, *supra* note 13, at 499–500.

Franklin, a former analyst who worked for the Office of the Secretary of the Department of Defense, provided the reports to Rosen and Weissman.[135] Similar to Gorin and Salich, Rosen and Weissman proffered the theory that the phrase "information related to the national defense" was unconstitutionally vague.[136] While the court conceded that the phrase was ambiguous, it determined that "information relating to the national defense" had previously been held to mean "government secrets" that could be potentially damaging to national security.[137] Because precedent established a definition, the court dismissed the defense, finding the term did not violate due process.[138]

The scope of what information is sufficiently related to the national defense is broad and wide-reaching, and has not been adequately defined through case law or otherwise.[139] There is no clear definition of what information falls under the definition of "national defense," and there is no incorporation of the currently used classification system that characterizes information the government determines needs special safeguarding.[140]

2. The Intent Requirement

Aside from the lack of clarity about what disclosures the Espionage Act applies to, the intent requirement in sections 793 and 794 add their own element of confusion. There are three intent standards in sections 793 and 794: an "intent or reason to believe," a willful disclosure, and a disclosure that injures the United States or is advantageous to a foreign nation.

a. Intent or Reason to Believe

The intent requirement in sections 793(a)–(b) and 794(a) further complicates the application of the Act, especially because the motivations for disclosing protected information have evolved over the last century.[141] Take the case of a

---

135. *Id.* Franklin was the initial divulger of the information and Rosen and Weissman were third-party recipients/publishers. *Id*.

136. *Rosen*, 445 F. Supp. 2d at 607.

137. *Id.* at 612, 622; *see also* Epstein, *supra* note 13, at 501 (discussing the *Rosen* case and that the Judge "reasoned that judicial precedent [had] limited and clarified 'information relating to the national defense' as any government secret, the unauthorized disclosure of which could threaten the national security.").

138. *Rosen*, 445 F. Supp. 2d at 622.

139. Edgar & Schmidt, *supra* note 15, at 986.

140. *See id.* (based on case law, "secrecy [may be] the litmus of defense-relatedness and thus put government classification at the fore, despite the multiplicity of purposes which secrecy in fact serves. The expansive reach of the term [information related to the national defense] leaves all-important whether *Gorin* was correct in regarding the statute's culpability formulation as adequate to fend off the dangers of overbreadth.").

141. *See generally* Goitein, *supra* note 9 ("Disclosures of classified information come in all different forms. On one end of the spectrum, there are acts of espionage designed to harm the country by providing highly sensitive information to any enemy. On the other end, there are revelations of government wrongdoing by patriotic public servants who carefully avoid any disclosure of truly sensitive information. And there is

proclaimed whistleblower who discloses protected information to the public in order to expose alleged government wrongdoing, rather than to injure the United States in any way.[142] If certain subsections of the Act require that the discloser intend to injure the United States, then such an argument seems an adequate defense.[143] The whistleblower's alleged subjective intent was not to injure the United States or aid a foreign government, but to inform the American public of perceived government wrongdoing.[144] However, there is no explicit whistleblower or "well-intentioned leaker" exception to the statute, so even subjective intent to expose wrongdoing puts the whistleblower in a position to have "reason to believe" that such a disclosure could harm national security.[145] Alternatively, if subjective intent is an appropriate defense, then a whistleblower defense could be a guise for a more evil intent.[146] A divulger need not be handled or recruited by a foreign government and may seek to collect information in an effort to aid a foreign government once he or she obtains something presumptively useful.[147] After all, there are established legal channels to disclose employer misconduct, although not comprehensively, which prevent sensitive information from reaching the hands of an adversary.[148] Whether or not "good faith" subjective intent is a valid defense to the "intent or reason to believe"

---

everything in between.").

142. *See e.g.* MELISSA GOODWIN ET AL., AMERICAN CIVIL LIBERTIES UNION, DISAVOWED: THE GOVERNMENT'S UNCHECKED RETALIATION AGAINST NATIONAL SECURITY WHISTLEBLOWERS 4, 10 (2007), *available at* https://www.aclu.org/sites/default/files/pdfs/safefree/disavowed_report.pdf [*hereinafter* DISAVOWED] (on file with the *McGeorge Law Review*) (highlighting that "whether a government employee decides to speak out is intensely personal – but almost all national security whistleblowers decide to disclose wrongdoing because they believe they have a patriotic duty to do so."). Conversely, an argument can be made that a whistleblower had specific intent to harm the U.S. government by exposing perceived government wrongdoing to the public in order to elicit outrage and promote change. *See generally* Walter Pincus, *A True Whistleblower Doesn't Behave Like Edward Snowden*, WASH. POST (June 2, 2014), http://www.washingtonpost.com/world/national-security/a-true-whistleblower-doesnt-behave-like-edward-snowden/2014/06/02/5e8484e0-e90c-11e3-afc6-a1dd9407abcf_story.html (on file with the *McGeorge Law Review*) (noting that "[a] real whistleblower would have selected the documents to be published, made certain they didn't harm security and remained in the country to face the consequences of his actions.").

143. *See generally* Edgar & Schmidt, *supra* note 15, at 987–88 (describing that "[i]f 'injury' is determined with reference to the actor's subjective perceptions, defenses are plausible in three common espionage situations. . . .").

144. *See* Goitein, *supra* note 9 (describing the various levels reasons for disclosures of classified information). However, it is important to note that in the case of Edward Snowden, his actions after the initial disclosure to the media, including taking protected information to foreign countries, could very well be considered aid to a foreign government. *See infra* Part III.D.1.

145. 18 U.S.C. §§ 793(a)–(b), 794(a) (2012).

146. *See* CHANGES IN ESPIONAGE, *supra* note 25, at 32, 70 (showing a differing in motives over time, but not discussing any "whistleblowing" or "well-intentioned" motive when it comes to committing "espionage").

147. *Id.*

148. *See supra* note 88 and accompanying text (regarding the various whistleblower protection statutes and their shortcomings); s*ee* Goitein, *supra* note 9 ("[T]he Whistleblower Protection Act . . . prohibits government agencies from taking adverse 'personnel actions' against whistleblowers. However, the Act excludes intelligence community employees, and it does not provide any whistleblower with a defense against criminal prosecution."); *see also* CRS REPORT FOR CONGRESS, *supra* note 81, at 1 (providing an overview of the Whistleblower Protection Act).

requirement, one thing is certain: the statute does not require the defendant to have acted in "bad faith."[149]

Although section 794(b) requires intent, the reach of the statute is much broader—the divulger need only "intent to communicate" protected information without any contemplation of any injury or result.[150] And under subsections 793(d)–(e), the scienter requirement is even more confusing because no showing of specific intent is required.[151]

When it comes to criminal intent under these subsections, prosecutors can demonstrate actual intent by proving one of two states of mind: purpose or knowledge.[152] Purpose is the act or desire to bring about a result,[153] while knowledge is the awareness that a result follows from an action.[154] Thus, one interpretation of the requisite intent is that the divulger must reveal information to another in some manner with the desire to injure the United States or with the knowledge that such conduct is likely to injure the United States.[155] Under such a broad reading, the whistleblower who acquires such information, for example, would clearly have intent or at the very minimum "reason to believe" that the recipient could use the information to a foreign advantage or to injure the U.S., because he is likely aware that such a result would follow from its revelation.[156] The same may be true in the case of a media publisher who obtains defense related information from a source.[157] As scholars have concluded, "Congress focused more on motive rather than result," thus "intend[ing] to distinguish revelation of defense information in espionage from the same revelation in public debate, on the basis of the intent to inform the public."[158] Presumably, the Act requires the same motive for the whistleblower who acquires defense information

149. *See* Statement of Vladeck, *supra* note 18, at 3 ("it is clear at the very least that nothing in the text of the statute speaks to the defendant's bad faith.").

150. 18 U.S.C. § 794(b); *see* Edgar & Schmidt, *supra* note 15, at 945 ("794(b) is somewhat broader [than 794(a)] because the required culpability is only the mere intent that information be communicated. The actor's state of mind with respect to the injurious consequences of the communication is irrelevant.").

151. The divulger only needs to "willfully communicate."18 U.S.C. § 793(c)–(d); *see infra* Part III.A.2.b (discussing "willfully").

152. *See* Edgar & Schmidt, *supra* note 15, at 989 (discussing the differences between "conscious purpose" and awareness).

153. BLACK'S LAW DICTIONARY 1431 (10th ed. 2014) (defining purpose as "[a]n objective, goal, or end," and defining purposeful as "[d]one with a specific purpose in mind; deliberate.").

154. *Id.* at 1003 (defining knowledge as "[a]n awareness or understanding of a fact or circumstance; a state of mind in which a person has no substantial doubt about the existence of a fact.").

155. Edgar & Schmidt, *supra* note 15, at 986–87, 989.

156. *See id.* at 987

> ("In most instances, however, people who make efforts to obtain defense-related information, whether journalists or spies, do so because they envision the possibility of communicating it to others. When the actor expects to tell others, the statute purports to make the acquisition criminal-depending upon whether the intended or predictable consequences of revelation are that the information will be used to injure the U.S. or to advantage any foreign nation.").

157. *Id.*

158. *Id.* at 989.

for public revelation.[159] It seems then that under such circumstances, courts should weigh motive greater than any resulting injury.[160]

The courts have taken several different approaches when interpreting the intent requirement,[161] but the Supreme Court last defined it directly in *Gorin v. United States*.[162] In *Gorin*, the Court determined that disclosure of information in violation of the Espionage Act must be made with "bad faith."[163] On the element of intent, the Court determined that the government must show the divulger acted in bad faith in order to find that he violated these subsections.[164] The few courts that later considered this issue have followed the Supreme Court's interpretation of intent in *Gorin*.[165]

The troublesome implications of the "reason to believe" definition of intent—knowledge that injury to the United States or aid to a foreign nation may occur—extend quite far.[166] Consider, again, a hypothetical whistleblower who has obtained actual "national defense information" concerning what he believed to be government misconduct. Even if he lacked specific intent to injure the United States, and all other elements of the statute are met, he almost certainly had reason to believe revelation could potentially injure the United States or aid a foreign government. Thus, awareness of the possible consequences is seemingly enough despite the fact that the divulger never specifically intended them.[167]

What Congress meant by "intent" or "reason to believe" in the statute is as unclear as the terms themselves.[168] While the legislative debate over 794(b)

---

159. *See generally* DISAVOWED, *supra* note 142 and accompanying text.

160. *See* Edgar & Schmidt, *supra* note 15, at 989

> ("Congress intended to distinguish revelation of defense information in espionage from the same revelation in the public debate, on the basis of the intent to inform the public. If a distinction under 793(a) and (b) is to be drawn between obtaining information for espionage and for publication, it should turn on the culpability of the motive, not on a strained construction of what ultimate consequences will ensue.").

Presumably, the same could apply to a whistleblower. *See generally id.* (describing congressional attempts to draw distinctions based on intent).

161. *See e.g.,* Pierce v. United States, 252 U.S. 239, 252 (1920) (giving little regard to the intent requirement, and finding that giving the words any other interpretation "unduly restricts the natural meaning of the clause, leaves little for it to operate upon, and disregards the context and the circumstances under which the statute was passed.").

162. Gorin v. United States, 312 U.S. 19, 28 (1941).

163. *Id.*

164. *Id.*

165. *See e.g.,* United States v. Rosen, 445 F. Supp. 2d 602, 643 (E.D. Va. 2006) (finding that the government must prove beyond a reasonable doubt that the defendants disclosed classified information in bad faith with actual intent to injure the United States); *see supra* notes 136–138 (discussing the facts of the case).

166. *See* Edgar & Schmidt, *supra* note 15, at 989, 997 (explaining that the term can be interpreted in at least two different ways: awareness of consequences or subjective purpose).

167. *See id.* at 991 ("There are accordingly serious problems with a construction of the 'reason to believe' phrase that would be satisfied by an awareness of possible forbidden consequences, as opposed to a conscious intent to bring them about.").

168. *Id.*

addressed the intent requirement in relation to other provisions later repealed,[169] the 793(a) and (b) record provides only two Congress Members' direct understanding of intent in the statute.[170] Congressman Edwin Webb interpreted intent to mean "a purpose to injure the United States,"[171] and Congressman George Graham interpreted intent as "a guilty purpose, to wit, to injure the United States."[172] While Congress might have equated intent with purpose,[173] it gave little attention to the interpretation of "reason to believe."[174] Arguably, this phrase is the most troublesome and controversial of these subsections' scienter elements.[175] Courts could read this phrase so broadly that it encompasses any cognizable consequence,[176] or they might interpret it narrowly and fail to adequately cover acts of espionage that, although not intended to injure or aid, have always been penalized under the Act.[177] In either case, courts will benefit from more accurate and unambiguous definitions so that they can effectively apply the statute's culpability requirement to initial divulgers.[178]

b. Willfully

Sections 793(d) and 793(e) do not require actual intent or reason to believe; rather, the divulger need only "willfully communicat[e]" information relating to the national defense to someone "not entitled to receive it."[179] While the legislative history provides little insight into what it means to willfully communicate,[180] courts have construed the term in many ways.[181] In *United States v. Morison,* prosecutors charged Samuel Morison, a former United States intelligence analyst, under sections 793(d) and 793(e) of the Espionage Act for sending classified satellite images of Soviet naval operations to Jane's Defence Weekly.[182] He was convicted on both counts in 1985.[183] On the element of intent,

169. *Id.*

170. *Id.* at 995–96.

171. 55 CONG. REC. 1071, 1591 (1917).

172. *Id.* at 1717–18.

173. Edgar & Schmidt, *supra* note 15, at 996.

174. *Id.* at 991; 55 CONG. REC. 1591 (1917).

175. *See* Edgar & Schmidt, *supra* note 15, at 996 (discussing the effect to be given to the interpretation of these subsections).

176. *Id.* at 991. For example, if a reporter intends to publish received classified information, he has reason to believe it could be used to injure the U.S. or aid a foreign nation.

177. *Id.* at 997. For example, someone who sells classified information to advantage a foreign nation purely to make money, completely indifferent to that result.

178. *See* Edgar & Schmidt, *supra* note 15, at 1076–77 (explaining that the "confusion about the culpability standards" of the Espionage Act requires "clarification by legislation.").

179. 18 U.S.C. 793(d)–(e) (2012).

180. Edgar & Schmidt, *supra* note 15, at 999.

181. *See e.g.,* United States v. Morison, 844 F.2d 1057, 1071 (4th Cir.1988), United States v. Kiriakou, 898 F. Supp. 2d 921, 926 (E.D.Va. 2012) (interpreting the term "willfully").

182. *Morison*, 844 F.2d at 1060–61.

183. James Risen*, Clinton Did Not Consult C.I.A. Chief on Pardon, Official Says,* N.Y. TIMES (Feb. 17,

the Fourth Circuit Court of Appeals upheld the District Court's instruction that "[a]n act is done willfully if it is done voluntarily and intentionally and with specific intent to do something the law forbids. That is to say, with a bad purpose either to disobey or to disregard the law."[184] Thus, the Government's burden of proof under sections 793(d) and (e) of the Act is to demonstrate that the divulger made the disclosure with a "bad purpose" or in "bad faith."[185]

In 2012, John Kiriakou, a former Central Intelligence Agency analyst, was convicted of espionage under section 793(d) for revealing a co-worker's classified name and information regarding the CIA's use of waterboarding interrogation techniques to the press.[186] One of his defenses was that he did not meet the necessary scienter element and could not be charged under the Act because he had a good faith basis for disclosing the information.[187] The court ultimately rejected the contention and found that, under the statutory language, the defendant's "salutary motive" was irrelevant; the government did not need to prove intent to injure as in 793(a) and (b).[188] All the government needed to show was that Kiriakou willfully communicated "information relating to the national defense which . . . the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation."[189] Kiriakou ultimately plead guilty to the charges, possibly because he was unable to show he lacked the intent to harm the United States.[190] Although the court did not specifically define "willfully," it seemed to infer that "willfully" did not mean intentionally, at least not in the sense that Kiriakou needed any particular motive to injure the United States.[191]

The same was true for the conviction against Bradley Manning in 2012.[192] Manning, a former United States Army private, disclosed more than 91,000 military-related, classified documents to Wikileaks.[193] In his prosecution,[194] the

---

2001), www.nytimes.com/2001/02/17/us/clinton-did-not-consult-cia-chief-on-pardon-official-says.html (on file with the *McGeorge Law Review*). Following his conviction, President Clinton pardoned Morison. *Id.*

184. *Morison*, 844 F.2d at 1071.

185. CRIMINAL PROHIBITIONS REPORT, *supra* note 16, at 16 n.99, 18.

186. *Kiriakou*, 898 F. Supp. 2d at 922; Scott Shane, *Ex-Officer is First From C.I.A. to Face Prison for a Leak,* N.Y. TIMES (Jan. 5, 2013), www.nytimes.com/2013/01/06/us/former-cia-officer-i-the-first-to-face-prison-for-a-classified-leak.html (on file with the *McGeorge Law Review*).

187. *Kiriakou*, 898 F.Supp.2d at 922.

188. *Id.* at 926–27.

189. 18 U.S.C. 793(d) (2013); *Kiriakou*, 898 F. Supp. 2d at 922.

190. *See generally* United States v. Kiriakou, No. 1:12cr127 (LMB), slip op. at 12 (E.D.Va. Oct. 16, 2012) (explaining why Kiriakou cannot raise a "good faith defense" to the charges under the Espionage Act).

191. *See Kiriakou*, 898 F. Supp. 2d at 923 (distinguishing the scienter requirements willfully and intentionally).

192. CRIMINAL PROHIBITIONS REPORT, *supra* note 16, at 3; Associated Press, *Manning Largely Barred from Discussing WikiLeaks Harm*, First Amendment Center (July 20, 2012), http://www.firstamendment center.org/manning-largely-barred-from-discussing-wikileaks-harm (on file with the *McGeorge Law Review*).

193. CRIMINAL PROHIBITIONS REPORT, *supra* note 16, at 2

194. Bradley Manning was prosecuted by a Military court martial. Julie Tate, *Judge Sentences Bradley Manning to 35 Years*, WASH. POST, Aug. 21, 2013, http://www.washingtonpost.com/world/national-

court found that his intent of allegedly informing the public of government wrongdoing was inadmissible.[195] Therefore, like Kiriakou, the court found the scienter element "willfully" requires no specific intent, so the well-intentioned defense was moot.[196] Manning ultimately received a thirty-five year prison sentence for violating section 793(e).[197]

The legislative history is uncertain as to what Congress specifically meant by "willfully," and why Congress chose that term rather than "intent" as in the other sections.[198] But one logical conclusion is that whatever definition the legislature meant to give to "willfully," it is distinctly different from "intent or reason to believe."[199] Scholars believe that "willfully" is a lower-threshold scienter requirement and is easier for the government to prove than specific intent.[200]

c. Injury of the United States or to the Advantage of Any Foreign Nation

Under subsections 793(a)–(e) and 794(a), the divulger must have "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."[201] Critics of this language point to the question of whether such a disclosure must actually injure the United States or advantage a foreign government or if it is enough that the divulger merely intended such a result.[202] Indeed, many defendants in recent leak cases have argued the theory that revealing classified information that results in no harm to national security cannot constitute espionage within the meaning of the Espionage Act.[203] Looking at the specific language of the statute, the divulger need only have the requisite intent to injure or advantage a foreign nation; such a

---

security/judge-to-sentence-bradley-manning-today/2013/08/20/85bee184-09d0-11e3-b87c-476db8ac34cd_story.html (on file with the *McGeorge Law Review*). A military court martial prosecuted Manning. *Id.*

195. Associated Press, *Manning Largely Barred from Discussing WikiLeaks Harm*, FIRST AMENDMENT CENTER (July 20, 2012), http://www.firstamendmentcenter.org/manning-largely-barred-from-discussing-wikileaks-harm (on file with the *McGeorge Law Review*).

196. *Id.*; *see supra* note 191 and accompanying text.

197. Tate, *supra* note 194.

198. Edgar & Schmidt, *supra* note 15, at 1038–39.

199. *Id*. at 1039.

200. GOVERNMENT SECRECY, *supra* note 51, at 37; *see* Edgar & Schmidt, *supra* note 15, at 1039 ("The Executive draftsmen of 793(d) and (e) clearly intended 'willful" to require a minimum culpable intent. Their concern was to close loopholes in the law, not impose stricter standards on the Government by requiring proof of illicit ulterior purpose.").

201. 18 U.S.C. §§ 793(a)–(e), 794(a) (2012).

202. *See* David Dishneau, *Witness: No Harm to US from Leaked Gitmo Files*, YAHOO NEWS, July 9, 2013, http://news.yahoo.com/witness-no-harm-us-leaked-gitmo-files-165619198.html (on file with the *McGeorge Law Review*) (discussing Bradley Manning's defense that he did not actually harm the U.S.).

203. *See id.* and accompanying text; *see also* United States v. Kim, Criminal No. 10-255 (CKK), slip op. at 10 (D.D.C. May 30, 2013) (regarding the theory that there was no injury to the U.S., and thus, no crime under the Espionage Act).

result need not actually manifest.[204] The fact that in some cases the leaked information results in little or no injury to the nation has brought this issue to light.[205]

Courts have focused on "advantage" rather than "injury" because under subsections requiring a scienter element, a defendant can more plausibly assert that he or she did not intend any sort of injury to the U.S.[206] Judicial interpretation of the phrase "advantage to a foreign government" is a source of confusion.[207] First, the plain meaning of "advantage" is "helpful," and given the nature of intelligence activities by other countries, courts likely could deem any information obtained by foreign countries as advantageous.[208] Second, to "any foreign nation" is likewise troublesome because the sensitivity or advantage of the information changes depending on which country has the information.[209] It appears that the statute does not require a foreign nation's advantage to be adversarial in nature; in fact, other subsections specifically use the term "enemy" and not "foreign nation," drawing a distinction between the terms.[210]

Recall that in *Gorin*, Salich provided United States counterintelligence reports on Japanese activities to the U.S.S.R.'s agent.[211] None of the reports contained information regarding United States military operations, installations, or preparedness as specifically proscribed in the Espionage Act.[212] Regardless, the information likely still related to the national defense,[213] and presumably could advantage a foreign nation.[214]

In *United States v. Morison*, the Fourth Circuit determined that the prosecution must "prove that the disclosure . . . would be potentially damaging to the United States or might be useful to an enemy of the United States."[215] The

---

204. 18 U.S.C. §§ 793(a)–(e), 794(a).

205. *See supra* notes 203–204 and accompanying text.

206. *See* Edgar & Schmidt, *supra* note 15, at 987 ("Only the 'advantage' aspect of the standard has received judicial elucidation.").

207. *Id.*

208. *Id.*

209. *See generally* Epstein, *supra* note 13, at 513–14 (discussing how "foreign nation" should be changed to "enemy" of the United States because "information disclosed to an enemy of the United States would inherently qualify under the 'could be used to the injury of the United States' clause.").

210. 18 U.S.C. §§ 793–794; *see generally* Epstein, *supra* note 13, at 514–15 ("Revision of the 'to the advantage of any foreign nation' clause is necessary because the disclosure of information to the advantage of key allies of the United States . . . could actually be beneficial in a time of war.").

211. 312 U.S. 19, 22–23 (1941).

212. *Id.*

213. Discussed *infra* Part III.D.4.

214. *Gorin*, 312 U.S. at 29. The Court also stated,

> "Nor do we think it necessary to prove that the information obtained was to be used to the injury of the United States. The statute is explicit in phrasing the crime of espionage as an act of obtaining information related to the national defense. . . . No distinction is made between friend or enemy."

Id. at 29–30.

215. 844 F.2d 1057, 1071 (1988).

court declined to adopt the defendant's argument that the national defense information must cause "actual damage," but still required the prosecution to show the information could "potentially" harm the United States or be beneficial to the enemy.[216]

However, one court recently addressed whether a leaker could successfully defend with the argument that no actual injury or advantage to a foreign nation could result from the leak.[217] In 2010, prosecutors charged Stephen Kim, a former senior analyst for the United States Department of State, under the Act for allegedly disclosing to a Fox News reporter that North Korea was planning to test a nuclear bomb.[218] A federal judge for the United States District Court of the District of Columbia ruled that "the court declines to construe section 793(d) to require the Government to show that the disclosure of the information at issue would be potentially damaging to the United States or might be useful to an enemy of the United States in order to satisfy the statutory requirement that the information relate to the 'national defense.'"[219] Effectively, the judge decided that the government need not address the injury at all.[220] This decision goes against the *Morison* court's interpretation, further illustrating the inconsistency with interpreting the troublesome language. Kim ultimately pled guilty to the charges.[221]

The language of the statute itself seems to suggest that a violation of the Espionage Act turns on the divulger's intent and not on the actual resulting harm.[222] However, whether the Act requires a divulger's actions actually harm the United States or provide an advantage to a foreign nation remains controversial.[223] Even though the language of the statute is largely straightforward, some critics of the Espionage Act argue that a leaker should only be convicted if harm to the United States actually resulted from the disclosure.[224]

---

216. *Id.* at 1072.

217. United States v. Kim, Criminal No. 10-255 (CKK), slip op. at 7, 10 (D.D.C. May 30, 2013).

218. Timothy M. Phelps, *Former State Department Official Pleads Guilty in Leak to Fox News*, LA TIMES (Feb. 7, 2014), http://articles.latimes.com/2014/feb/07/nation/la-na-rosen-plea-20140208 (on file with the *McGeorge Law Review*).

219. Memorandum Opinion, United States v. Kim, Criminal No. 10-255 (CKK) (D.D.C. May 30, 2013).

220. *Id.*

221. Phelps, *supra* note 218.

222. 18 U.S.C. 793(a)–(e), 794(a) (2012).

223. *See e.g.* United States v. Kim, Criminal No. 10-255 (CKK), slip op at 7 (D.D.C. May 30, 2013). Associated Press, *Manning Defense Rebuts Evidence Leaks Caused Harm*, MILITARY.COM (July 9, 2013), http://www.military.com/daily-news/2013/07/09/manning-defense-rebuts-evidence-leaks-caused-harm.html (on file with the *McGeorge Law Review*) (discussing the Manning case and whether or not leaks resulted in harm to the U.S.).

224. *See supra* note 204–205 and accompanying text.

IV. A PROPOSAL TO CHANGE THE ESPIONAGE ACT

> *"I understood what I was doing and the decisions I made. However, I did not truly appreciate the broader effects of my actions. . . . I am sorry for the unintended consequences of my actions. When I made these decisions, I believed I was [going to] help people, not hurt people."*
>
> *—Bradley Manning*[225]

Many of the inconsistencies in the Espionage Act jurisprudence stem from the Act's imprecise terminology, lack of clear definitions, and uncertain legislative intent.[226] As a result, defendants have challenged the Act as unconstitutionally vague,[227] grossly overbroad, and inconsistently interpreted.[228] In order to effectively prosecute cases of legitimate espionage and other criminal conduct under its provisions, including divulgence of information that impacts the nation's security, revision is paramount.[229]

A. Scope of Information Related to the National Defense

One solution to help effectively protect the national defense is to specify what information really matters.[230] This requires narrowing and defining particular categories of information that are critical to national security.[231] The breadth of the term "related to the national defense" creates a great deal of uncertainty, and in fact, encompasses less truly sensitive information than it would if properly defined.[232]

Scholars have noted that adding the term "classified information" to define the phrase, or replacing the phrase with "classified information," would help narrow the overly broad phrase "related to the national defense" and help remove vagueness,[233] primarily because properly classified information must only be done so in protection of national security.[234] Categorizing information as

---

225. Matt Sledge, *Bradley Manning Takes Stand: 'I Am Sorry . I Believed I Was Gonna Help People,'* HUFFINGTON POST (Aug. 14, 2014, 6:21 PM), www.huffingtonpost.com/2013/08/14/bradley-manning-sorry_n_3757490.html (on file with the *McGeorge Law Review*) (including the transcript of Bradley Manning's unsworn statement during his sentencing hearing on August 14, 2013).

226. *See e.g.* Edgar & Schmidt, *supra* note 15, at 1076 (arguing that "the basic espionage statutes are totally inadequate. Even in their treatment of outright spying they are poorly conceived and clumsily drafted.").

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

228. *See e.g.* Edgar & Schmidt, *supra* note 15, at 1076–77 (explaining varying interpretations of the statutory language).

229. *See id.* at 1079 (elucidating need for revision).

230. *See id.* at 1081 (explaining that important issues should not be "treat[ed] . . . so opaquely").

231. *See id.* at 1085 (advocating for narrower application).

232. *Id*. (discussing the "vague parameters of 'national defense information'").

233. Patricia L. Bellia, *Wikileaks and the Institutional Framework for National Security Disclosures,* 121 YALE L.J. 1448, 1522 (2012).

234. *See* INFORMATION SECURITY OVERSIGHT OFFICE, MARKING CLASSIFIED NATIONAL SECURITY INFORMATION 2 (rev. ed. 2014), *available at* http://www.archives.gov/isoo/training/marking-booklet.pdf

classified generally distinguishes sensitive information critical to the national defense,[235] but it should not be dispositive. First, overclassification is a problem in the United States,[236] and many documents that would have negligible consequences to national security may nonetheless be improperly classified.[237] Second, not all critical national defense information is classified under the United States classification system, but may consist of closely held information or even observable acts.[238] Thus, classified information should be a factor in determining what information relates to the national defense, but should not be the only test. Further, the statute should explicitly define "classified information" in order to clarify what it encompasses.[239]

The Act also protects information that may not be considered classified, but remains sensitive or necessarily protected for purposes of national security.[240] Such information should also be explicitly defined in the statute, but narrower than "related to the national defense." Congress should add and define the term "sensitive information" alongside "classified information."[241]

At the very minimum, Congress should remove the term "national defense" because it is outdated.[242] Since September 11, 2001 and the creation of the

---

[hereinafter MARKING CLASSIFIED] (on file with the *McGeorge Law Review*) ("Information shall not be classified for any reason unrelated to the protection of national security.").

235. GOVERNMENT SECRECY, *supra* note 51, at 27 n.4.

236. Bellia, *supra* note 233, at 1524 (noting that "not all unauthorized leaks are responses to overclassification, [but] both the Pentagon Papers case and the WikiLeaks disclosures provide evidence of the phenomenon"). Additionally, there is no defense for overclassification or "improper classification" when facing criminal liability. *Id.* at 1523.

237. *See* MARKING CLASSIFIED, *supra* note 234, at 2 ("Information shall not be classified for any reason unrelated to the protection of national security.") *See generally* Bellia, *supra* note 233, at 1524 (explaining that "[o]ne can sympathize with the claim that some of the material ought not to have been classified while still having discomfort with this process of 'declassification' as well as the elimination of deference to the executive's judgment that disclosure would potentially cause harm.").

238. Edgar & Schmidt, *supra* note 15, at 979–80. For example, observing how many vehicles leave a military base can provide information on capability, strength, numbers of soldiers, etc. all of which could be critical to the national defense. *See id.* at 979 (commenting "several small clues may permit piecing together the entire story"). Another example is the aggregation of several pieces of unclassified information to deduce sensitive or classified information. *Id*.

239. The Espionage Act already contains an explicit definition for "classified information" in subsection 798(b). 18 U.S.C. § 798 (2012). It is defined as "information which, at the time of a violation of this section, is for reasons of national security, specifically designated by a United States Government Agency for limited or restricted dissemination or distribution." *Id.* Another statute specifically defines "classified information of the United States" in a way that may be helpful to the reform of the Espionage Act as "information originated, owned, or possessed by the United States Government concerning the national defense or foreign relations of the United States that has been determined pursuant to law or Executive order to require protection against unauthorized disclosure in the interests of national security." *Id.* § 1924(c).

240. ALICE R. BUCHALTER ET. AL, LIBRARY OF CONGRESS, LAWS AND REGULATIONS GOVERNING THE PROTECTION OF SENSITIVE BUT UNCLASSIFIED INFORMATION 10 (2004), *available at* http://www.loc.gov/rr/frd/pdf-files/sbu.pdf (on file with the *McGeorge Law Review*).

241. One way of defining sensitive information may be "information in which the United States has demonstratively taken steps to safeguard."

242. *See* MARKING CLASSIFIED, *supra* note 234, at 2 (using the term "national security" as the distinguishing characteristic for classifying information that needs safeguarding).

Department of Homeland Security, the modern lexicon has been "homeland security" or "national security."[243] There are very distinct differences between the terms "national defense" and "national security"—one implies defending the nation whereas the other implies securing or protecting the nation.[244] Since "national security" is the more defined and commonly used term, the broad term "national defense" only complicates the modern understanding of the Espionage Act.

Lastly, the Act references specific documents and types of information throughout its subsections; for example, subsection 793(a) protects "information concerning any vessel, aircraft," etc.[245] While some of these examples may themselves be broad or even outdated,[246] greater specificity will limit the scope of sensitive information. Thus, Congress should reevaluate these specific areas of information to determine whether they remain vital to national security.

B. Defining Existing Terms

If Congress wishes to keep the Espionage Act in its current form, then defining confusing terms is essential to ensure appropriate prosecutions.

1. Intent Element

The "intent or reason to believe" element should be changed to "malicious intent or actual knowledge." While actual knowledge would seemingly always apply to government employees with security clearance, like Snowden, who undoubtedly know that disclosures of Top Secret information are likely to injure the United States,[247] such specific language makes absolutely clear that those who have valid access to classified information have no excuse. They will, at a minimum, have "actual knowledge" that such disclosure could "injure the United States or aid a foreign government." Such specificity will also ensure that those who do not possess security clearances and secondary recipients like the media[248]

---

243. *See e.g.,* DEP'T HOMELAND SECURITY, HOMELAND SECURITY INFORMATION NETWORK, http://www.dhs.gov/homeland-security-information-network (last visited Nov. 1, 2014) (on file with the *McGeorge Law Review*) (demonstrating that "homeland security" is not only an entire government department, but also a widely understood term).

244. The former implies prevention; the latter implies reaction.

245. 18 U.S.C. §§ 793–794 (2012).

246. *See e.g.* 18 U.S.C. § 793(a) (specifying the term "camp" as a protected type of information—a term that is very broad generally, yet extremely narrow in comparison to other military installations currently in existence).

247. Persons who possess a valid federal security clearance and are indoctrinated for access to classified information, and are required to sign a nondisclosure agreement setting forth the requirements of secrecy and the penalties if they are not adhered to, fully informing the person of consequence of espionage. INFO. SEC. OVERSIGHT OFFICE, CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT, STANDARD FORM NO. 312 (rev. ed. 2013) (prescribed by 32 C.F.R § 2001.80 (2010).) (on file with the *McGeorge Law Review*).

248. Epstein, *supra* note 13, at 515 n.254 (citing Bruce Fein, *Pelosi's Chance to be Lady Liberty*, Wash. Times, Nov. 14, 2006, at A17).

are not punished when they merely had some "reason to believe" the information had potentially injurious effects to the United States.[249] The Act imposes an extremely harsh sentence on those who merely had "reason to believe" that their disclosures would injure the United States or aid foreign governments.[250] The Act should not apply to them in the same way it would be applied to someone with malicious intent or actual knowledge.[251] Additional clarity could help deter potential leakers who likely do not understand what the prosecution must prove in order to convict a defendant of espionage;[252] indeed, many likely have the "traditional spy" notion in mind and may not identify themselves as such.[253]

"Willfully" should be specifically defined and distinguished from "intent." If Congress wants courts to interpret willfully as a lesser standard of culpability than intent, then Congress should define willfully as "consciously" or "knowingly."[254] If Congress intends courts conflate willfully with intent, then Congress should specify that willfully means purposeful (intent to bring about a desired result).[255]

2. Injury to the United States or Advantage of any Foreign Nation

Since "injury to the United States or advantage of any foreign nation" could broadly cover any disclosure—even disclosures that cause little or no injury[256]—Congress should articulate or define these terms more accurately. Specifically, Congress should replace "foreign nation" with "enemy of the United States,"[257] and then define enemy under applicable law.[258] It makes little sense that an individual would have reason to believe that helpful information provided to an ally would consequently injure the United States, especially when such disclosure may be in the interest of the United States.[259] Thus, some information may not injure the United States and, in fact, may even advantage the United

249. 18 U.S.C. § 793 (2012).

250. *Id.*

251. *Id.*

252. *See generally* Bellia, *supra* note 233, at 1522 (stating that "reform involves reassessing how the law should deter and respond to leaks").

253. *See supra* Part III.A. (discussing the different categorizations for divulging information).

254. Most courts that have addressed the issue have viewed the term "willfully" to mean less than intent, so such an interpretation would be more consistent with case law. *See supra* Part III.B.2 (discussing the scienter element of the Espionage Act). A proposed revision would be to specifically write into the Act: "For Purposes of this Act, 'willfully' is defined as knowledge or awareness the result will follow."

255. A proposed revision would be to specifically write into the Act: "For Purposes of this Act, 'willfully' is defined as intentionally, with purpose to bring about a desired result."

256. *See supra* Part III.B.1.c. (regarding the problems with injury to the U.S.).

257. Epstein, *supra* note 13, at 513.

258. *Id.* (proposing that "enemy" should be defined as "anyone who could qualify as a lawful or unlawful enemy combatant under the Military Commissions Act of 2006.").

259. *Id*. at 514 (quoting Judge Learned Hand) ("[The Espionage Act] as enacted necessarily implies that there are some kinds of information 'relating to the national defense' which must not be given to a friendly power, not even to an ally, no matter how innocent, or even commendable, the purpose of the sender may be.").

States.[260] However, courts would find it extremely difficult to assess such an assertion.[261] In addition, other information may be sensitive but not classified or may be improperly classified because it does not relate to United States national security or national defense.[262] If it is unrelated to national security—the entire purpose of the Espionage Act—then an individual could not have reason to believe it would injure the United States. Consequently, the information must actually touch on the national defense in order for the divulger to have reason to believe that it could cause any injury.[263]

C. Expanding the Nature of Disclosure

In addition to defining certain terms, Congress should re-write the statute to encompass acts that currently do not constitute espionage. Take, for example, media publication or whistleblowing revelation through proper channels.[264] The Act should provide a defense if a defendant can demonstrate that he or she made the disclosure through proper whistleblowing reporting channels, which consequently resulted in a public disclosure. Clearly, this defense would not cover Snowden-style straight-to-press disclosures, but such a defense may encourage future whistleblowers to report through the proper channels. If a well-intentioned whistleblower seeks to reveal government wrongdoing, then allowing the appropriate avenues and a suitable defense may help limit the exposure of information that could have damaging effects to national security or advantage an adversary and facilitate transparency.

V. CONCLUSION

The Espionage Act needs revision to remove confusion and create a more consistent application of the law. In order to effectively prosecute legitimate cases of espionage, courts and prosecutors must clearly understand what constitutes espionage. Overly broad and ambiguous terminology has resulted in confusion, misapplication of the statute, and constitutional challenges.[265] If Congress truly desires an Act that protects our national security, it must

---

260. *See id.* and accompanying text.

261. *See id.* at 514–515 (discussing advantages of disclosures to the United States' allies during war).

262. *See* Bellia, *supra* note 233 (noting that "not all unauthorized leaks are responses to overclassification, [but] both the Pentagon Papers case and the WikiLeaks disclosures provide evidence of the phenomenon"); MARKING CLASSIFIED, *supra* note 234, at 2 ("Information shall not be classified for any reason unrelated to the protection of national security."); note 236 and accompanying text.

263. *See supra* section IV.B (providing suggestions to revision of the scope of information related to the national defense).

264. *See, e.g.,* Intelligence Cmty. Whistleblower Prot. Act of 1998, H.R.B. 3694, 105th Cong. §§ 702–03 (1998) (enacted). This Act "protects intelligence community whistleblowers who follow detailed procedures for disclosing matters of 'urgent concern,' a category that includes evidence of flagrant law breaking and lying to Congress." Bellia, *supra* note 233 at 1525.

265. *See supra* notes 226–228 and accompanying text.

adequately encompass modern developments, such as technology and the classification system, to refine the antiquated law. Our espionage laws should comport with modern reality. Application of the statute in charging whistleblowers, leakers, and potentially others will only prove more challenging as the country develops new technologies. Congress must suitably address the issues the Act has raised.