WHISTLE WHILE YOU (RE)WORK IT: CONGRESS'S DUTY TO AMEND THE ESPIONAGE ACT OF 1917

Annah Seaford*

* Annah Seaford is a third-year student at George Mason University's Antonin Scalia Law School in Arlington, Virginia. She graduated from Appalachian State University in 2021 with a B.A. in Political Science. Annah is a member of the National Security Law Journal, the Vice President of Communications for the Criminal Law Society, and a student advisor for the Mason Veterans and Servicemembers Legal Clinic.

INTRODUCTION

Edward Snowden is arguably one of the most infamous whistleblowers in American history, if not the most infamous. His name carries household weight, and his actions have been depicted by Hollywood.[1] Snowden was an intelligence contractor for the National Security Agency ("NSA"),[2] known for disclosing classified NSA surveillance programs.[3] After deciding that he wanted to inform the public about those programs, he flew to Hong Kong and contacted reporters from *The Guardian*,[4] who conducted and published his interviews.[5] Snowden also gave consent to publish his name, declining the protection of anonymity.[6] In his telling, Snowden wanted to release the information because he felt that the actions of the United States, creating a "surveillance machine," would eventually eliminate privacy.[7] In June 2013, following his disclosures, he was charged under the Espionage Act of 1917.[8] The United States tried to extradite and prosecute him, but he fled to Russia.[9] Snowden now has Russian citizenship, which he was granted in September 2022.[10] After Snowden's leaks, President Obama suggested transparency reforms, even going so far as to suggest reforming parts of the Patriot Act and the Foreign Intelligence Surveillance Court.[11]

---

[1] *See* SNOWDEN (Open Road Films 2016).
[2] *See Edward Snowden, National Security Whistleblower,* NATIONAL WHISTLEBLOWER CENTER (Apr. 8, 2018), https://www.whistleblowers.org/whistleblowers/edward-snowden/.
[3] *See id.*
[4] *See id.*
[5] *See id.*
[6] *See* Glenn Greenwald, *Edward Snowden: The Whistleblower Behind the NSA Surveillance Revelations,* THE GUARDIAN (Jun 11, 2013), https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance.
[7] *See id.*
[8] *See Edward Snowden, supra* note 2.
[9] *See id.*
[10] *See* Charles Maynes, *Putin Grants Russian Citizenship to Edward Snowden*, NPR (Sept. 26, 2022, 1:10 PM), https://www.npr.org/2022/09/26/1125109303/putin-edward-snowden-russian-citizenship.
[11] *See Edward Snowden, supra* note 2.

The Espionage Act was designed to address traditional espionage—think of spies like James Bond.[12] This Act was not designed for individuals who attempt to tell the public what the government is doing—public whistleblowers—yet these individuals are often the ones prosecuted under it.[13] While this type of "espionage" began in the 1970s and 1980s,[14] the government has recently started to take more aggressive action when leaks occur.[15] Ironically, the government may be aware of some of these leaks before the public, and it is possible that they may be encouraging some of them.[16] Additionally, the government has a hand in how or when certain information is published.[17] The government often uses the media to control leaks or spin the narrative to satisfy its own policy.[18] For instance, The *New York Times* refrained from posting a story regarding nuclear weapons in Cuba at the request of President Kennedy.[19] Improvements to the Espionage Act are desperately needed to distinguish between whistleblowers and traditional spies. Doing so will necessarily increase protections for whistleblowers.

This Comment explores the unconstitutional and impractical aspects of the Espionage Act. The current language of Section 793 poses constitutional threats to due process[20] and adversely impacts public policy. A constitutional threat arises from the vagueness of the phrase "relating to the national defense" as used throughout the

[12] *See* Geoffrey R. Stone, *Judge Learned Hand and the Espionage Act of 1917: A Mystery Unraveled*, 70 U. CHI. L. REV. 335, 336 (2003).
[13] *See* Juliana Kim, *Sen. Rand Paul Wants to Repeal the Espionage Act Amid the Mar-a-Lago Investigation*, NPR (Aug. 15, 2022, 5:00 AM), https://www.npr.org/2022/08/15/1117457622/rand-paul-what-is-espionage-act-repeal.
[14] *See* Jereen Trudell, *The Constitutionality of Section 793 of the Espionage Act and Its Application to Press Leaks,* 33 WAYNE L. REV. 205, 208 (1986).
[15] *Id.* at 208-09; *see also* Sharon LaFraniere, *Math Behind Leak Crackdown*, N.Y. TIMES (July 20, 2013), https://www.nytimes.com/2013/07/21/us/politics/math-behind-leak-crackdown-153-cases-4-years-0-indictments.html.
[16] *See* Mary-Rose Papandrea, *The Publication of National Security Information in the Digital Age,* 5 J. NAT'L SEC. L. & POL'Y 119, 121 (2011).
[17] *See id.*
[18] *See id.*
[19] *Id.*
[20] *See* 18 U.S.C. § 793 (referencing the ambiguity of the term "national defense").

statute.[21] Due to the statute's vagueness, activities that may not ordinarily be criminal can fall under § 793. For instance, would merely talking about a foreign nation's activities against the United States fall under the Act? The Act itself is unclear on this point. Thus, the current language of § 793 of the Espionage Act must be amended to rectify the constitutional problem as well as the public policy concerns associated with this section.

This Comment will also explore other statutes and legal frameworks that affect whistleblowers. It will detail some well-known whistleblowers, their actions, and how the law was applied to them. In doing so, this Comment will examine the difficulty of trying to "strik[e] the right balance between necessary secrecy in a dangerous world and the need for an informed citizenry in a democracy."[22]

Part I of this Comment provides background information about whistleblowers. Part II focuses on the legal framework applicable to them, and how it works in practice. Part II also discusses how the statute has been applied to infamous leakers. Part III provides an analysis of both constitutional and policy issues that could arise from prosecuting whistleblowers under § 793 of the Espionage Act. Part IV describes proposed legislation and similar changes to the protections afforded to intelligence community whistleblowers. Part V summarizes the issue and concludes with proposed solutions.

Intelligence community whistleblowers should be given stronger protections. They are currently protected under the Intelligence Authorization Act for Fiscal Year 2014 and Presidential Directive 19 ("PPD-19"), which some believe afford weaker protections relative to the Whistleblower Protection Act.[23] Whistleblowers may also fall under § 793 of the Espionage Act of 1917 ("Espionage Act"), which encompasses "gathering, transmitting, or losing defense information."[24] This section applies when

[21] *Id.*

[22] STEPHEN DYCUS ET AL., NATIONAL SECURITY LAW, 1234 (7th ed. 2014).

[23] *See FAQ Whistleblower Protection Act,* NATIONAL WHISTLEBLOWER CENTER (June 7, 2022), https://www.whistleblowers.org/faq/whistleblower-protection-act-faq/.

[24] 18 U.S.C. § 793(d).

whistleblowers do not appropriately disclose information to the proper authority, but instead make unauthorized disclosures.[25]

In certain contexts, whistleblowers should be protected even though they may be committing a crime. At present, no statute governing whistleblowers provides any such protections, regardless of significant governmental overreach, illegal conduct by public officials, or any other public interest concerns.[26] Thus, there are two hypothetical paths to reform the Espionage Act. The first solution entails passing additional legislation about whistleblowers and their legal protections. Passing additional legislation would likely be difficult to achieve, and, given the complexity of the issues addressed, and the sheer number of statutes that touch on whistleblowing and leaking,[27] may do little to clarify the problems identified herein. Thus, the better solution is for Congress to consolidate and amend the current statutory scheme so that it better protects whistleblowers' Constitutional rights.

I. "WHISTLEBLOWER" DEFINED

A whistleblower is a person who "reports waste, fraud, abuse, corruption, or dangers to public health and safety to someone who is in the position to rectify the wrongdoing."[28] Similarly, a leak is "(i) a targeted disclosure, (ii) by a government insider (employee, former employee, contractor) (iii) to a member of the media, (iv) of confidential information the divulgence of which is generally proscribed by law, policy of convention (v) outside of any formal process (vi) with an expectation of anonymity."[29] While there is a

[25] *See generally* 18 U.S.C. § 793; Intelligence Authorization Act for Fiscal Year 1999, Pub. L. No. 105-272, 112 Stat. 2396 (1998); Whistleblower Protection Act 5 U.S.C. § 2302(b)(8) (1989); RODNEY M. PERRY, CONG. RSCH. SERV., R43765, INTELLIGENCE WHISTLEBLOWER PROTECTIONS: IN BRIEF, 1 (Oct. 23, 2014).

[26] *See* Stephen I. Vladeck, *The Espionage Act and National Security Whistleblowing after Garcetti*, 57 AM. U. L. REV. 1531, 1542 (2008).

[27] *See generally* Intelligence Authorization Act for Fiscal Year 1999, Pub. L. No. 105-272, 112 Stat. 2396 (1998); 5 U.S.C. § 2302(b)(8); Perry, *supra* note 25, at 1.

[28] *What is a Whistleblower,* NATIONAL WHISTLEBLOWER CENTER, https://www.whistleblowers.org/what-is-a-whistleblower/ (last visited Oct. 10, 2022).

[29] David E. Pozen, *The Leaky Leviathan: The Government Condemns and Condones Unlawful Disclosures of Information*, 127 HARV. L. REV. 512, 521 (2013).

distinction in definition, due to colloquial language stemming from popular culture and media, this Comment will consider those who leak information as "whistleblowers," though there is some controversy over whether only unauthorized disclosures qualify as leaks.[30] An authorized disclosure is "frequently the result of a planned strategy by a government official to advance or promote a particular policy, sabotage the plans or policies of rival agencies or political parties, discredit opponents, float a public opinion trial balloon, or expose corruption or illegal activities."[31] The authorized leak may or may not be publicly acknowledged, and the government may even condone approved leaks.[32]

Employers cannot retaliate against an employee who makes a disclosure protected by law.[33] Intelligence Community whistleblowers are simply employees of a federal intelligence agency who disclose evidence of misconduct by the agency.[34] The Intelligence Community consists of 18 different organizations.[35] These organizations are broken into three different categories: independent agencies, Department of Defense intelligence components, and offices within other departments of agencies.[36] The two independent agencies are the Office of the Director of National Intelligence and the Central Intelligence Agency.[37] There are nine Department of Defense intelligence components, including the NSA, Defense Intelligence Agency, National-Geospatial-Intelligence Agency, and National Reconnaissance Office.[38] There are also intelligence arms within the armed forces branches (the Army, Navy, Marine Corps, Air Force, and Space Force).[39] The remaining seven intelligence community

[30] *See id.*
[31] *See* Papandrea, *supra* note 16, at 121.
[32] *See id.*
[33] *See Making Lawful Disclosures*, OFF. OF THE DIR. OF NAT'L INTEL., https://www.dni.gov/index.php/who-we-are/organizations/icig/icig-related-menus/icig-related-links/making-lawful-disclosures (last visited Sept. 27, 2023).
[34] *See* Perry, *supra* note 25, at 1.
[35] *See Members of the IC*, OFF. OF THE DIR. OF NAT'L INTEL., https://www.dni.gov/index.php/what-we-do/members-of-the-ic (last visited Sept. 28, 2023).
[36] *See id.*
[37] *See id.*
[38] *See id.*
[39] *See id.*

members are parts of other departments or agencies.[40] These include the Office of Intelligence and Counter-Intelligence within the Department of Energy, the Office of Intelligence and Analysis in the Department of Homeland Security, U.S. Coast Guard Intelligence, the Federal Bureau of Investigation ("FBI") within the Department of Justice, the Office of National Security Intelligence in the Drug Enforcement Agency, the Bureau of Intelligence and Research in the Department of State, and the Office of Intelligence and Analysis in the Department of Treasury.[41]

II. WHISTLEBLOWING STATUTES AND OTHER LEGAL FRAMEWORK

This Comment will not conduct a deep dive on the intricacies of the host of whistleblowing statutes currently in place; however, it is necessary to briefly summarize a few of them. Many different statutes address whistleblowing, because there is no consolidated whistleblower law.[42] Individuals who leak information may be protected, but whether, and to what extent, they are immunized depends on how they leak the information; to whom; and the nature of the information itself.[43] Whistleblowers who leak intelligence information have limited rights due to the nature of their job and their access to sensitive information.[44]

A. *Whistleblower Protection Act*

One key statute that establishes whistleblower protections is the Whistleblower Protection Act ("WPA").[45] The WPA, part of the Civil Service Reform Act of 1978,[46] generally protects whistleblowers employed by the federal government.[47] However, it does not extend to any whistleblowers who are part of the intelligence community or

[40] *See id.*
[41] *See Members of the IC, supra* note 35.
[42] *See What Journalists Need to Know About Whistleblowers,* NATIONAL WHISTLEBLOWER CENTER, https://www.whistleblowers.org/what-journalists-need-to-know-about-whistleblowers/ (last visited Oct 1, 2023).
[43] *See id.*
[44] *See id.*
[45] *See FAQ Whistleblower Protection Act, supra* note 23.
[46] *See id.*
[47] *See id.*

those who work for the FBI.[48] The WPA protects public disclosure of "a violation of any law, rule, or regulation . . . if such disclosure is not specifically prohibited by law *and* if such information is not specifically required by Executive order to be kept secret in the interest of national defense or the conduct of foreign affairs."[49]

B. *Espionage Act of 1917*

The Espionage Act of 1917 was born in an era in which the United States government was concerned with containing and limiting the criticisms of its efforts, including espionage, in World War I.[50] Notably, The Espionage Act was designed to allow President Wilson to either "censor or punish" those who gave away national security information.[51] The government sought to protect its citizens and punish those who acted in a way that "endangered the peace, welfare, and honor of the United States."[52] In other words, the Act represented an attempt to maintain secrecy when it came to national security issues.[53] However, Congress struggled to craft language that would protect the nation's defense secrets from spies without "promulgating broad prohibitions that would jeopardize the legitimate efforts of citizens to seek information and express views concerning national security."[54] In the years following its enactment, many uses of the Act raised free speech issues.[55] Government leaks became more common later on, rising to prominence in the 1970s and 1980s.[56] Today, there is greater focus on individuals with access to

[48] *See id.*
[49] *See* Vladeck, *supra* note 26, at 1537.
[50] *See* Scott Bomboy, *The Espionage Act's Constitutional Legacy*, NAT'L CONST. CTR BLOG, (AUG. 17, 2023), https://constitutioncenter.org/blog/the-espionage-acts-constitutional-legacy.
[51] Mary-Rose Papandrea, *National Security Information Disclosures and the Role of Intent,* 56 WM. & MARY L. REV. 1381, 1395 (2015).
[52] Trudell, *supra* note 14, at 206.
[53] *See id.* at 208.
[54] *See* Harold Edgar & Benno C. Schmidt, Jr., *The Espionage Statutes and Publication of Defense Information*, 73 COLUM. L. REV. 929, 939 (1973).
[55] *See* Bomboy, *supra* note 50.
[56] *See* Trudell, *supra* note 14, at 208.

sensitive materials disclosing information that they believe shows government malfeasance or misfeasance.[57]

The current issues with the Espionage Act center relate to the First Amendment and the difficulties inherent in determining whether an individual has proper authority to disseminate information.[58] The First Amendment states that "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances."[59] Though the Espionage Act of 1917 was "directed primarily towards such matters as espionage and the protection of military secrets," its use and misuse also pertains to freedom of speech when it limits individuals' ability to disclose, and therefore the public's ability to learn of, and criticize, the government's activities.[60]

Section 793 of the Espionage Act is titled "Gathering, transmitting, or losing defense information."[61] There are many subparts to this section, all of which relate to the dissemination of national defense information to and from unauthorized persons.[62] Subsection A states that "[w]hoever, for the purpose of obtaining information respecting the national defense with intent or reason to believe that the information is to be used to the injury of the United States, or to the advantage of any foreign nation" will be fined or sentenced to ten years in prison.[63] Subsection B largely restates Subsection A (that an individual seeking to obtain national defense information could face fines or imprisonment) but it also incorporates an "intent or reason to believe" standard.[64] Subsection C also reiterates the previous two subsections in including the required purpose and

[57] *See* Bomboy, *supra* note 50.
[58] *See* Bomboy, *supra* note 50.
[59] U.S. Const. amend. I.
[60] Stone, *supra* note 12, at 336.
[61] 18 U.S.C. § 793.
[62] *See id.*
[63] *Id.* § 793(a).
[64] *See id.* § 793(b) (describing that the intent or reason to believe standard relates to the information that one may intend or reasonably believe could injure the United States or aid a foreign nation).

reason to believe standards, but also adds "attempts to receive information that relates to the national defense,"[65] encapsulating more activity. Furthermore, subsection D directly states:

> Whoever, lawfully having possession of, access to, control over, or being entrusted with any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign national, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it on demand to the officer or employee of the United States entitled to receive it . . . shall be fined under this title or imprisoned not more than ten years, or both.[66]

Subsection E is very similar to Subsection D because the 1950 amendment of the Espionage Act essentially split Subsection D into two parts.[67] Subsection E, however, details those who have "unauthorized possession" of national defense information which could either be used to injure the United States or give an advantage to a foreign nation, which again can encapsulate a broader scope of activity.[68] The individual must also have either willfully communicated or retained the information.[69] The *mens rea* requirement in the "reason to believe" standard is specified in most subsections of § 793.[70] This makes it illegal to disclose any information "to any person not entitled to receive it."[71]

[65] *See id.* § 793(c).
[66] *Id.* § 793(d) (emphasis added).
[67] *See* Edgar & Schmidt, *supra* note 54, at 1021.
[68] *See* 18 U.S.C. § 793(e).
[69] *See id.*
[70] *See id.* § 793(a)-(d).
[71] *Id.* § 793(d).

C. *The Defense Secrets Act*

The Defense Secrets Act was Congress's first attempt to protect military information by way of legislation.[72] The Defense Secrets Act is similar to the Espionage Act, but the former focuses more exclusively on the military.[73] Both statutes, however, utilize vague wording that leave many finer points unclear.[74] For example, the Defense Secrets Act established vague statutes regarding activities around military installations that related to gathering information.[75] The Defense Secrets Act also created severe punishments for those who gave a foreign government illegally-obtained information.[76] The punishments imposed under the act do not vary on the basis of the perpetrator's knowledge or intent.[77] Furthermore, because the Espionage Act is very closely related to the Defense Secrets Act, some of the same language was carried over.[78] For example, Subsections 793 A and B of the Espionage Act crib from the Defense Secrets Act language describing ways to gather information.[79] However, the Defense Secrets Act "lacked the important requirement of intent to injure the United States or advantage a foreign nation."[80] Thus, the language of Subsections D and E of § 793, described above, is also incorporated, which can pose interpretative problems.[81]

D. *Presidential Policy Directive-19*

President Obama signed Presidential Policy Directive 19 in 2012.[82] Titled *Protecting Whistleblowers with Access to Classified Information,* this directive was the first executive branch protection

---

[72] *See id.*, at 939–40.
[73] *See* Edgar and Schmidt, *supra* note 54, at 940.
[74] *See id.*; 18 U.S.C. § 793.
[75] *See* Edgar and Schmidt, *supra* note 54, at 940.
[76] *See id.*
[77] *See id.*
[78] *See id.*
[79] *See* Edgar and Schmidt, *supra* note 54, at 940.
[80] *Id.*
[81] *See id* (describing how the statute's failure to define "national security" creates these problems).
[82] *See* MICHAEL E. DEVINE, CONG. RSCH. SERV., R45345, INTELLIGENCE COMMUNITY WHISTLEBLOWER PROVISIONS, 1, 8 (2022).

regarding intelligence community whistleblowers.[83] However, PPD-19 only covers *some* intelligence community employees.[84] PPD-19 defined a protected disclosure as:

> a disclosure of information by the employee to a supervisor in the employee's direct chain of command up to and including the head of the employing agency, to the Inspector General of the employing agency or Intelligence Community Element, to the Director of National Intelligence, to the Inspector General of the Intelligence Community, or to an employee designated by any of the above officials for the purpose of receiving such disclosures, that the employee reasonably believes evidences (i) a violation of any law, rule, or regulation; or (ii) gross mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety.[85]

PPD-19 is limited. It prevents employees in the Intelligence Community from retaliation if they make a disclosure that is considered lawful.[86] An act of retaliation could be, but is not limited to, a demotion, transfer, suspension, or reassignment.[87] PPD-19 requires that a process be initiated for intelligence community employees who think they are suffering a reprisal due to a lawful disclosure.[88] Once this process is initiated, the Inspector General for the relevant agency will determine if there were any reprisals, and if there were, that Inspector General will make a recommendation of how to address the problem.[89] While the Inspector General makes such recommendations, the agency head, in reviewing the actions, is not required to accept any such recommendation.[90]

PPD-19 also mandates that intelligence community agencies establish a review process that would allow employees to appeal actions that would restrict their security clearance and ability to view sensitive information.[91] The whistleblower may request an external

[83] *See id.* at 8.
[84] *See id.*
[85] *Id.*
[86] *See id.*
[87] *Id.*
[88] DEVINE, *supra* note 89, at 9.
[89] *Id.*
[90] *Id.*
[91] *Id.*

review, conducted by the Intelligence Community Inspector General ("ICIG"), upon completing the agency review process.[92] The ICIG must provide annual reports to the congressional intelligence committees as to the ultimate disposition of their findings, which includes any actions they recommend.[93] Finally, the executive branch must "provide training to employees with access to classified information."[94] This does not include government contractors or members of the military.[95]

E. *The Intelligence Community Whistleblower Protection Act*

The Intelligence Community Whistleblower Protection Act ("ICWPA") was adopted in 1998.[96] ICWPA encourages congressional oversight.[97] The Act attempts to protect whistleblowers within the intelligence community, who, as noted above, are not covered by the Whistleblower Protection Act.[98] The ICWPA does not include protections for those serving in the military.[99]

ICWPA was a response to the problems created by the absence of a statutory whistleblower protection for members of the intelligence community. The absence of such a protection inhibited the necessary "flow of information" to those tasked with conducting oversight.[100] Under ICWPA, intelligence community members can report to the Inspector General of their intelligence community agency, so long as it regards "urgent concern[s]."[101] An urgent concern can be one of three things.[102] First, an "urgent concern" may be "a serious or flagrant problem, abuse, violation of law or executive order, or deficiency relating to the funding, administration, or operation of an intelligence

[92] *Id.*
[93] DEVINE, *supra* note 89, at 9.
[94] *Id.*
[95] *Id.*
[96] *See id.* at 2.
[97] *See id.* at 5.
[98] DEVINE, *supra* note 89, at 2.
[99] *See id.* at 2.
[100] *See id.* at 3.
[101] *Id.* at 2.
[102] DEVINE, *supra* note 89, at 2–3.

activity, involving classified information, but does not include differences of opinion concerning public policy matters."[103] Second, an "urgent concern" may be "a false statement to Congress, or willful withholding from Congress, on an issue of material fact relating to the funding, administration, operation of an intelligence activity."[104] Finally, an "urgent concern" may be "an action . . . constituting reprisal or threat of reprisal . . . in response to employee reporting an urgent concern."[105] While reprisal is an "urgent concern," ironically no language in ICWPA protects whistleblowers from reprisal.[106]

F. *Title VI of the Intelligence Authorization Act for Fiscal Year 2014*

Title VI of the Intelligence Authorization Act for Fiscal Year 2014 ("Title VI") was codified on July 7, 2014.[107] This was the first statutory framework that protected whistleblowers against reprisal actions stemming from their protected disclosure.[108] The content of this statute otherwise mirrors those of prior whistleblower protection statutes.[109]

G. *Constitutional Amendments*

This Comment discusses two constitutional amendments that relate to the Espionage Act: the Fifth and Fourteenth Amendments. The Fifth Amendment, in relevant part, states that "no person shall be . . . deprived of life, liberty, or property, without due process of law."[110] The Fourteenth Amendment has a similar clause that states, "[n]o State shall . . . deprive any person of life, liberty, of property, without

[103] *Id.* at 2–3.
[104] *Id.* at 3.
[105] *Id.*
[106] *Id* at 5.
[107] *Id* at 9.
[108] DEVINE, *supra* note 89, at 9.
[109] *See id.* at 2–3, 9.
[110] U.S. CONST. amend. V.

due process of law."[111] Thus, these amendments are commonly described as the "Due Process Clauses."[112]

The Supreme Court in, *Connally v. General Construction Co.*, established a related doctrine based on the Due Process Clauses.[113] *Connally* stands for the proposition that, when an ordinary person would not be able to understand a statute, it is unconstitutionally vague.[114] Similarly, in *Smith v. Goguen*, the Court reexamined the vagueness doctrine and concluded that, when an individual cannot discern whether conduct is acceptable or prohibited, the statute's vagueness renders it unconstitutional.[115]

H. *Espionage Act Cases*

While few cases dissect the Espionage Act, there are a few cases of importance. In *Gorin v. United States*, for example, the defendant was accused of taking information about certain activities occurring in the United States.[116] Gorin was accused of buying reports from another individual that described "Japanese activities in the United States."[117] The defendant argued that the phrase "relating to the national defense," not explicated in the statute, was "violative of due process because of indefiniteness."[118] The Court, however, accepted the government's definition of national defense, which it found was "a generic concept of broad connotations, referring to the military and naval establishments and the related activities of national preparedness."[119] The Court then convicted the defendant based on the Espionage Act's language requiring either that an individual acted in bad faith or that the information could hurt the United States or advantage a foreign nation.[120]

---

[111] U.S. CONST. amend. XIV.
[112] *See* U.S. CONST. amends. V, XIV (note that both contain the phrase "due process").
[113] *See generally* Connally v. Gen. Constr. Co., 269 U.S. 385, 390–91 (1926).
[114] *See id.* at 391.
[115] *See* Smith v. Goguen, 415 U.S. 566, 571–72 (1974).
[116] *See* Gorin v. United States, 312 U.S. 19, 22–30 (1941).
[117] *Id.* at 22.
[118] *Id.* at 23.
[119] *See id.* at 28.
[120] *See id.*

Similarly, the defendant in *United States v. Morison* released information and images of naval ships to a publication.[121] He was then charged with violating the Espionage Act.[122] While the jury convicted the defendant of violating the Espionage Act, the jurors were given extra-statutory instructions as to the definition of "national defense."[123] Notably, one member of the Fourth Circuit's three-judge panel thought that the jury instructions were the deciding factor for the case, and that without them, § 793 would be unconstitutionally vague and overbroad.[124]

In a more recent case, the district court in *United States v. Rosen* followed the logic of the majority in *Morison*.[125] The defendants in *Rosen* were accused of conspiring to transmit information related to national defense.[126] The defendants worked at the American Israel Public Affairs Committee without security clearance.[127] One of the defendants, Rosen, communicated with a foreign official stating that he had "picked up an extremely sensitive piece of information."[128] The two then discussed the information and, later other classified information.[129] The court denied the defendants' motion to dismiss the charges on the ground that the statute was vague; it reasoned that, although non-government employees had never been prosecuted under the statute before, the defendants' activities fell within the offense described therein, and the prosecution was not such a "novel" application of the statute that the defendants lacked fair notice that what they did was illegal.[130]

[121] *See* United States v. Morison, 844 F.2d 1057, 1061 (4th Cir. 1988).
[122] *See id.* at 1060–62.
[123] *See id.* at 1062, 1082.
[124] *See id.* at 1086 (Philips, J. concurring).
[125] *See generally* United States v. Rosen, 445 F. Supp. 2d 602 (E.D. Va. 2006).
[126] *See id.* at 607.
[127] *See id.* at 607–08.
[128] *Id.* at 608.
[129] *See id.*
[130] *Id.* at 629.

I. *Application of Whistleblower Laws to Infamous Whistleblowers*

Society has mixed feelings about those who reveal information.[131] The dichotomy comes from those who believe that information disclosures are imperative to society and those who believe disclosures negatively impact national security.[132] Some believe these individuals are traitors; however, regardless of society's beliefs, unauthorized disclosures have a long history of informing the public about nefarious and questionable governmental activities.[133]

1. Edward Snowden

Edward Snowden is one of the most known whistleblowers in United States history. Snowden was an intelligence contractor for the NSA.[134] In 2013, he disclosed classified programs run by the NSA and its British equivalent.[135] As previously mentioned, Snowden flew to Hong Kong, where he contacted *The Guardian*.[136] *The Guardian* thereafter conducted and published interviews with Snowden, detailing the classified programs that Snowden described.[137] *The Guardian* revealed Snowden's identity with consent.[138] Snowden said that he did not want the protection of anonymity,[139] and that he had no intention of hiding who he was because he thought he had done nothing wrong.[140] His motive for releasing the information was "to inform the public as to that which is done in their name and what which is done against them."[141] He felt he had to release the

[131] *See* A.W. Geiger, *How Americans have viewed government surveillance and privacy since Snowden leaks,* PEW RESEARCH CENTER, (June 4, 2018), https://www.pewresearch.org/short-reads/2018/06/04/how-americans-have-viewed-government-surveillance-and-privacy-since-snowden-leaks/.
[132] *Id.*
[133] *See* DYCUS ET AL., *supra* note 22, at 1234.
[134] *See Edward Snowden*, *supra* note 2.
[135] *See id.*
[136] *See id.*
[137] *See id.*
[138] *See* Greenwald, *supra* note 6.
[139] *See id.*
[140] *See id.*
[141] *See id.*

information because the United States government's actions had eroded its citizens' privacy.[142] His goal was to establish transparency, and he carefully chose each piece that was released.[143] Snowden believes that the NSA's surveillance programs violate the United States Constitution.[144] When he first started working for the government, he had to sign a nondisclosure agreement.[145] After breaching that agreement, Snowden said that it was like signing a pledge of allegiance, but to protect the Constitution from its enemies.[146]

In June 2013, Snowden was charged with espionage in violation of the Espionage Act of 1917.[147] His charges fell under §793(d) of the Act.[148] The United States government unsuccessfully tried to extradite Snowden after he fled to Russia.[149] Snowden has remained in Russia since then.[150] Russia's president, Vladimir Putin, granted him Russian citizenship in September of 2022.[151] After Snowden's leak, President Obama suggested transparency reforms for government agencies and their programs, which included "updating sections of the Patriot Act and reforming the Foreign Intelligence Surveillance Court."[152] The reforms included parts of the Patriot Act and the Foreign Intelligence Surveillance Court.[153]

Congress established the Foreign Intelligence Surveillance Court ("FISC") in the Foreign Intelligence Surveillance Act ("FISA")

---

[142] *See id.*
[143] *See id.*
[144] *See* Dave Davies, *Edward Snowden Speaks Out: 'I Haven't and I Won't Cooperate with Russia',* NPR, (Sept. 19, 2019), https://www.npr.org/2019/09/19/761918152/exiled-nsa-contractor-edward-snowden-i-haven-t-and-i-won-t-cooperate-with-russia.
[145] *See* Davies, *supra* note 151.
[146] *See* Davies, *supra* note 151.
[147] *See Edward Snowden*, *supra* note 2.
[148] *See* Catherine Taylor, *Freedom of the Whistleblowers: Why Prosecuting Government Leakers under the Espionage Act Raises First Amendment Concerns,* 74 NAT'L LAW. GUILD REV. 209 (2018).
[149] *See id.*
[150] *See id.*
[151] *See* Maynes, *supra* note 10.
[152] *See Edward Snowden*, *supra* note 2.
[153] *See* Maynes, *supra* note 10.

of 1978.[154] The FISC is intended to "protect classified national security information" by removing sensitive matters from traditional federal courts.[155] The FISC consists of federal judges appointed by the Chief Justice of the Supreme Court.[156] The court primarily rules on Fourth Amendment issues that are highly classified.[157] However, per the USA FREEDOM Act of 2015, the court must make its interpretations available to the public.[158]

2. Chelsea Manning

Chelsea Manning is also best classified a whistleblower, as she disclosed hundreds of thousands of records detailing the Iraq and Afghanistan wars.[159] Manning was court-martialed and sentenced to thirty-five years in prison, but only served seven.[160] Manning released the infamous "Collateral Murder" video, which depicted American soldiers shooting, wounding, and ultimately killing Iraqi civilians.[161] The video, along with the release of the records, led to her arrest.[162] The leak was posted to *Wikileaks*, an organization whose stated goal is "to bring information to the public."[163] Whatever the merits of her disclosure, Manning, as a member of the military, was not guaranteed

[154] *See Foreign Intelligence Surveillance Court (FISC)*, ELECTRONIC PRIVACY INFORMATION CENTER, https://epic.org/foreign-intelligence-surveillance-court-fisc/ (last visited Oct. 30, 2022).
[155] *See id.*
[156] *See id.*
[157] *See id.*
[158] *See id.*
[159] *See* Dave Davies, *Chelsea Manning Shared Secrets with WikiLeaks. Now She's Telling Her Own Story*, NPR (Oct. 17, 2022), https://www.npr.org/2022/10/17/1129416671/chelsea-manning-wikileaks-memoir-readme.
[160] *See id.*
[161] *See* Stuart Jeffries, *README.txt by Chelsea Manning Review- the Analyst Who Altered History,* THE GUARDIAN (Oct. 24, 2022, 4:00 AM), https://www.theguardian.com/books/2022/oct/24/readmetxt-by-chelsea-manning-review-analyst-who-altered-history-army-whistleblower.
[162] *See id.*
[163] Wikileaks, *What is WikiLeaks*, (May 7, 2011), https://www.wikileaks.org/About.html.

any statutory protections for blowing the whistle on the Collateral Murder video or anything else contained in those records.[164]

3. Current Public Opinion

Both sides of the political aisle have recently discussed the Espionage Act. For instance, former Democrat Representative Tulsi Gabbard introduced a bill titled the "Protect Brave Whistleblowers Act of 2020."[165] She proposed several changes, including reforming the intent requirements and adding an affirmative defense.[166] Unfortunately, her proposed bill never made it to the floor for a vote.[167]

Republicans have also been critical of the Act. Senator Rand Paul recently called for repealing the Espionage Act entirely.[168] He believes that the Act is not being enforced as originally intended.[169] His call followed closely on the FBI's raid of Donald Trump's Mar-a-Lago estate."[170] In this incident, FBI investigators removed classified documents from Trump's home; as of this writing, he faces prosecution for mishandling government records.[171] Now that former President Donald Trump has been indicted and charged under the Espionage Act, Republican Senator Lindsey Graham also believes the Espionage Act is not enforced as intended; in his words, because "[Trump] is not a spy; he did not commit espionage."[172] Senator Graham stated that the Espionage Act charges are "ridiculous" and contrasted the previous individuals charged under the Espionage Act: have been "people who turned over classified information to news

[164] *See* Intelligence Authorization Act For 1999, Pub. L. No. 105-272, 112 Stat. 2396 (1998); *see* Whistleblower Protection Act, 5 U.S.C. § 2302(b)(8) (1989); *see* Cong. Rsch. Serv., R43765, Intelligence Whistleblower Protections: In Brief, 1 (2014).
[165] *See generally* Protect Brave Whistleblowers Act of 2020, H.R. 8452, 116th Cong. (2020).
[166] *See* Protect Brave Whistleblowers Act of 2020, H.R. 8452, 116th Cong. §2(a)(1), §799(B) (2020).
[167] *See generally* Protect Brave Whistleblowers Act of 2020, H.R. 8452, 116th Cong. (2020).
[168] Kim, *supra* note 13.
[169] *Id.*
[170] *Id.*
[171] *Id.*
[172] *See* Zachary B. Wolf, *Trump is not a spy. Why is he charged under the Espionage Act?,* CNN (June 13, 2023), https://www.cnn.com/2023/06/13/politics/espionage-act-trump-what-matters/index.html.

organizations to hurt the country or provide it to a foreign power", which he asserts that Trump did not do.[173]

III. REQUIREMENTS AND PUBLIC POLICY CONCERNS

Congress must amend the Espionage Act of 1917 in three ways. First, Congress must amend § 793 to prevent it from being unconstitutionally vague. To address the unconstitutionally vague phrases, language should be added that explicitly defines "national defense." While Congress does not need to exactly copy the definition from other codes, adding a definition could be instrumental in clarifying the scope and application of § 793.[174] Second, Congress should introduce a specific intent requirement to target those who act with bad intent in trying to harm the United States. Finally, Congress should add an affirmative defense to § 793 strictly for individuals who leak information to the public about matters that relate to society as a whole. An affirmative defense is a set of facts that mitigate or lessen the consequences of the defendant's action.[175] It allows the defendant to justify why he or she committed the crime.[176]

A. *The Espionage Act is Unconstitutionally Vague*

One of the most significant concerns about the Espionage Act is that "national defense" and "related to national defense" are never explicitly defined, despite their uses throughout it.[177] These terms are arguably unconstitutionally vague under the due process guarantees found in the Fifth and Fourteenth Amendments.[178] A statute or act is unconstitutionally vague unless it defines the conduct proscribed such that the average person is able to discern what is permissible and what

---

[173] *Id.*

[174] *See* 10 U.S.C 8720(1) (noting there are "national defense" definitions).

[175] *See* National Association for Legal Support, *Affirmative Defenses,* (June 21, 2017), ttps://www.nals.org/blogpost/1359892/279125/Affirmative-Defenses.

[176] *Id.*

[177] *See* 18 U.S.C. § 793 (noting the absence of a definition for "national defense".); *see* 10 U.S.C 8720(1) (establishing that Congress is capable of defining "national defense" in other settings).

[178] *See* U.S. Const. amend. V (establishing that no one will be "deprived of life, liberty or property without due process of law); *see* U.S. Const. amend. XIV (describing that no State shall "deprive any person of life, liberty, or property, without due process of law.")

is prohibited.[179] Vagueness is "directed at lack of sufficient clarity and precision in the statute."[180] Section 793 contains vague terms when it uses numerous variations of "national defense" in different contexts.[181] Examples include "information respecting the national defense;" "anything connected with the national defense," and "information relating to the national defense."[182] How does one know exactly what information would relate to the national defense? Does a national security law textbook contain information that is related or connected to national defense?[183] Possibly so, given that the author discusses national security and defense issues.[184]

There is little case law that defines the vague phrases "relating to national defense" and "connected to national defense," which gives little guidance to prospective whistleblowers, administration officials, and judges.[185] Similarly troubling, if read broadly, the "reason to believe" standard may allow prosecution when an merely individual knows that an action will occur based on the circumstances.[186] When statutes are vague, they "may encourage arbitrary and discriminatory enforcement."[187]

Additionally, if these subsections are taken literally, they must constitute a violation of the Fifth and Fourteenth Amendments.[188] Many acts can be criminalized by relying on the phrase "related to the national defense."[189] Thus, Congress could not have meant exactly what they wrote when they codified § 793, and the only way to fix the error is to amend § 793 to include specific definitions of these vague words and phrases. One may suggest that the best way to address the exact meaning of the § 793 is to turn to previous Espionage Act

---

[179] *See* Connally v. General Constr. Co., 269 U.S. 385, 391 (1926); *but see* Smith v. Goguen, 415 U.S. 566, 572 (1974).
[180] United States v. Morison, 844 F.2d 1057, 1070 (4th Cir. 1998).
[181] *See generally* 18 U.S.C. § 793.
[182] 18 U.S.C. § 793(a)–(d).
[183] *See generally* DYCUS, ET AL., *supra* note 22.
[184] *Id.*
[185] *See* Edgar and Schmidt, *supra* note 54, at 986.
[186] *See* Edgar and Schmidt, *supra* note 54, at 989.
[187] United States v. Rosen, 445 F. Supp. 2d 602, 617 (E.D. Va. 2006).
[188] *See* U.S. CONST. amends. V, XIV (suggesting that the literal nature of these words violates Due Process Clause found in both amendments).
[189] *See* 18 U.S.C. § 793.

jurisprudence. That, however, is not practical as there have only been a handful of cases dealing with the Espionage Act, "limited almost entirely to spies," which means that the application of those cases to twenty-first century challenges is equally unclear.[190]

There are a few cases that are relevant to this analysis and remain influential in how the Espionage Act is brought to trial. For example, the Supreme Court ruled in *Gorin v. United States* that the limiting words within the section are not too vague and are subject to requiring "intent or reason to believe that the information to be obtained is to be used to the injury of the United States, or the advantage of any foreign nation."[191] In *Gorin*, the defendant was accused of gathering information coming from the Naval Intelligence Branch detailing ongoing Japanese activities in the United States.[192] The Court also said that the Espionage Act "requires those prosecuted to have acted in bad faith" and the "sanctions apply only when scienter is established."[193] The defendant was convicted because he acted with intent or reason to believe that the information obtained could either hurt the United States or be used to the advantage of any foreign nation.[194] The Court avoided having to explicitly define "national defense" because they relied on the fact that the leaks injured the United States and advanced the interests of a foreign nation.[195] If they had to rely on the definition of "national defense" in the Espionage Act, there would have been a massive problem. Namely, because there is no definition of what "relates to the national defense" in the section.[196]

In *Gorin*, the Court used the government's suggested definition of "national defense" as a "generic concept of broad connotations, referring to the military and naval establishments and

---

[190] *See* Greg Myre, *Once Reserved for Spies, Espionage Act Now Used Against Suspected Leakers,* NPR (June 28, 2017, 8:07 AM), https://www.npr.org/sections/parallels/2017/06/28/534682231/once-reserved-for-spies-espionage-act-now-used-against-suspected-leakers.
[191] *See* Gorin v. United States, 312 U.S. 19, 27-28 (1941).
[192] *See id.* at 29–30.
[193] *Id.* at 28.
[194] *See id.*
[195] *See id.*
[196] *See* 18 U.S.C. § 793 (noting the absence of a definition for "national defense".)

related activities of national preparedness."[197] Even so, the government relied on basic assumptions of broad terms. Additionally, other statutes define the term "national defense."[198] 10 U.S.C. § 8720 (1) defines national defense as "the needs of, and the planning and preparedness to meet, essential defense, industrial, and military emergency energy requirements relative to the national safety, welfare, and economy, particularly resulting from foreign military or economic actions."[199] Thus, if Congress can define "national defense" in other chapters, they can amend § 793 to include a more specific definition that is not overinclusive.

Similarly, the *Morison* court ignored the question of applying the vagueness doctrine, a doctrine that states if something is vague then it is unenforceable, of the Espionage Act in *United States v. Morison.*[200] Morison worked at the Naval Intelligence Support Center, handling top secret information.[201] He did off-duty work with a publication that dealt with international naval operations.[202] After one discussion, Morison offered to give the publication more information regarding an explosion near a naval base, which the publication accepted.[203] Later, he gave drawings and pictures of naval ships to the publication, which were published.[204] He was subsequently charged with violating the Espionage Act.[205] While he was ultimately convicted, Judge Phillips thought it was evident that these statutes were overly broad and imprecise.[206] Morison was convicted because the jury instructions imposed limiting language, which the court found permissible and, therefore not vague.[207]

Judge Phillips, concurring in *Morison*, believed that the language of § 793 was unconstitutionally vague.[208] He indicated that

---

[197] Gorin, 312 U.S. at 28.
[198] *See, e.g.,*10 U.S.C. § 8720 (1).
[199] 10 U.S.C. § 8720 (1).
[200] *See generally* United States v. Morison, 844 F.2d 1057 (4th Cir. 1988).
[201] *See id.* at 1060.
[202] *See id.*
[203] *See id.* at 1060–61.
[204] *See id.* at 1061.
[205] *See id.* at 1061–63.
[206] *See* Morison, 844 F.2d at 1085 (Philips, J., concurring).
[207] *See id.* at 1073 (majority opinion).
[208] *See id.* at 1085–86 (Philips, J., concurring).

the only reason he affirmed the decision was that the jury received clear jury instructions.[209] Moreover, he was concerned that since there are no limits on the reach of national security prosecution, this could perpetuate more criminal convictions for issues that are marginally related to national defense.[210]

In *United States v. Rosen*, the court references the *Morison* decision, alleging that there is a judicial limitation.[211] The court argues that the limitation imposed in the jury instructions about the intent with which the information is dispersed is sufficient to limit the phrase "information relating to the national defense."[212] However, *Rosen* relies on *Morison's* jury instruction limitations, which are judicially created, rather than relying on the statute itself.

If the vagueness continues, it would not only be bad law, but bad policy as well. For instance, the current political divides may create a reason for abusing the Espionage Act.[213] In recent years, there has been more outrage with how the Espionage Act is vague and overbroad. Senator Rand Paul wrote that the Espionage Act "was abused from the beginning to jail dissenters of World War I. It is long past time to repeal this egregious affront."[214] Some people are worried that each administration selectively picks which leaks are considered threats to national security.[215] While Senator Rand Paul suggests repealing the entire Espionage Act, going that far may not be necessary. When concerns are over what is a threat to national security, the answer should be to explicitly define the vague words in the Espionage Act.

---

[209] *See id.* at 1086.
[210] *See id.*
[211] *See* United States v. Rosen, 445 F. Supp. 2d 602, 621 (E.D. Va. 2006).
[212] *Id.*; s*ee also* United States v. Morison, 844 F.2d 1057, 1074 (4th Cir. 1988).
[213] *See* Robert D. Epstein, *Balancing National Security and Free-Speech Rights: Why Congress Should Revise the Espionage Act*, 15 COMMLAW CONSPECTUS 483, 486, 506 (2007).
[214] *See* Kim, *supra* note 13.
[215] *Id.*

B. *Specific Intent*

Motive and intent behind the disclosure plays a big role in the legal outcome for the individual. When malice is missing, there cannot be a successful conviction.[216] The Supreme Court has said that "innocence of intention will defeat a charge even of treason."[217]

There are many reasons that an individual would leak information. Some of these include financial pressure, a desire for policy change, or connections to a foreign government.[218] Additionally, the individual may want to sway public opinion or reveal illegal government behavior.[219] Some of those reasonings aren't necessarily nefarious in nature. Furthermore, there is no settled, definite law that states whether motive is legally significant.

For example, in *United States v. Rosen*, the court held that the "reason to believe" language of § 793 of the Espionage Act, "requires the government to demonstrate the likelihood of defendant's bad faith purpose to either harm the United States or to aid a foreign government."[220] When disclosures are done with a nefarious intent, these individuals deserve punishment.[221] Alternatively, this should mean that when disclosures are done without a nefarious intent, so as to not harm the United States, the individuals do not deserve punishment. Introducing the requirement of specific intent into the elements of the crime is essential in protecting whistleblowers as well as distinguishing them from traitors.

Legislative history also shows that Congress did not intend alternative interpretations of the meaning of § 793, or that the culpability requirements of particular subsections of § 793 were not satisfied if the individual was engaging in public debate or criticizing

---

[216] *See* Morissette v. United States, 342 U.S. 246, 262 n.21 (1952) (citing Haupt v. United States 330 U.S. 631 (1947).
[217] *Id.*
[218] *See* Karen E. Smith, Unauthorized Disclosure: Can Behavioral Indicators Help Predict Who Will Commit Unauthorized Disclosure of Classified National Security Information? (June 2015) (M.A. thesis, Naval Postgraduate School).
[219] *See* Dycus ET AL, *supra* note 22, at 1234.
[220] United States v. Rosen, 445 F. Supp. 2d 602, 626 (E.D. Va. 2006).
[221] *See* Papandrea, *supra* note 51, at 1383.

defense policy.[222] Therefore, motive does matter. Motive matters more so when dealing with the individual's public opinion after the information is released. For instance, the motive behind leaks can affect whether the media portrays them as "whistleblowers" or alternatively, as "traitors."[223]

When done to reveal what the government is doing to society as a whole, adding an affirmative defense to negate those motives is consistent with the legislative history[224]. Furthermore, some members of Congress believed that to be convicted, it must be done with "a conscious purpose to injure" the United States.[225]

C. *Affirmative Defense*

Edward Snowden would qualify for the affirmative defense because he leaked information regarding the NSA's plans to collect American phone metadata and content.[226] There must be a socially acceptable, compelling reason that the individual leaked certain information to qualify for the affirmative defense. Judge Wilkinson in *Morison* said that "national security is public security, not government security from informed criticism."[227] Snowden's reasons should be considered compelling because the NSA was capable of collecting phone data on nearly all Americans and was collecting "the content of emails, photos, and other media from the servers of nine Internet service companies (Microsoft, Google, Apple, Yahoo, AOL, Facebook, YouTube, Skype, and Paltalk)."[228] These secret programs were surveilling ordinary Americans and would fall under the proposed affirmative defense protections regarding public disclosures of social matters as a whole.

---

[222] *See* Edgar and Schmidt, *supra* note 54, at 991.
[223] *See* Papandrea, *supra* note 51, at 1437.
[224] *See* Edgar and Schmidt, *supra* note 54, at 994–998.
[225] *See* Edgar and Schmidt, *supra* note 54, at 995.
[226] *See* Constitutional Rights Foundation, *Edward Snowden, The NSA, and Mass Surveillance,* 10, 11 (2016), https://www.crf-usa.org/images/pdf/gates/snowden_nsa.pdf.
[227] *See* United States v. Morison, 844 F.2d 1057, 1081 (4th Cir. 1988) (Wilkinson, J. concurring).
[228] *See* Constitutional Rights Foundation, *supra* note 233.

Adding an affirmative defense to the Espionage Act is the best way to add whistleblower protections, while still acknowledging that the individual committed a crime. The leaker is simply saying that while they did commit a crime, there was a good reason to commit the crime.[229] Like all other defendants asserting affirmative defenses, the whistleblower must carry the burden to meet the standard of proof required.[230] This Comment does not propose that all whistleblowers should get off scot-free. Leaks happen often,[231] though the scale of the information may vary greatly.

Congress should amend the Espionage Act to include an affirmative defense when individuals publicly leak issues that impact all of society. Doing so would strike an appropriate balance between holding individuals responsible for their actions while also offering a reduction in legal consequences. This is a compromise that both sides of the political aisle should be able to agree on.[232]

Furthermore, jurisprudence surrounding the Espionage Act should turn to the First Amendment for more legal support. Rulings about freedom of speech from the Supreme Court show that a certain intent is required for some crimes.[233] For example, the Court held that actual malice was required to successfully prove libel against a public figure.[234]

IV. PROPOSED LEGISLATION

One author suggests amending the Espionage Act in a way that would exempt whistleblowers from prosecution after leaking

[229] *See* National Association for Legal Support, *supra* note 182.
[230] *See id.*
[231] *See* POZEN, *supra* note 29, at 528.
[232] *See* KIM, *supra* note 13; *see* Protect Brave Whistleblowers Act of 2020, H.R. 8452, 116th Cong. (2020).
[233] *See* PAPANDREA, *supra* note 51 at 1383.
[234] *New York Times Co. v. Sullivan*, 376 U.S. 254, 283 (1964).

information to the media,[235] which is a sentiment echoed in Representative Gabbard's proposed affirmative defense.[236]

Adding an affirmative defense would better balance the interest of whistleblowers and the United States's security. It allows the individual to be held responsible for their actions while also maintaining that there was a valid reason for leaking information.[237] In using an affirmative defense if the defendant goes to trial, he is accepting responsibility for his actions.[238] To not prosecute the leaker at all does not allow the individual to take responsibility for his actions, regardless of whether he would have gone to prison for his actions or not.

As mentioned above, Representative Gabbard introduced a bill known as "Protect Brave Whistleblowers Act of 2020."[239] In this bill, she proposed amending § 793 of the Espionage Act so that it becomes a specific intent crime.[240] In Subsection A, she suggests replacing "with intent or reason to believe" to "with specific intent."[241] For Subsection B, she suggests deleting "or reason to believe" and adding "that has been properly classified that is" to follow after "of anything."[242] Subsection C proposed revision, like B, includes adding "that has been properly classified that is" after "anything."[243] For Subsection D, she added the phrase: "and with specific intent to injure the United States or to advantage any foreign nation."[244] The exact language proposed for Subsection D is suggested for Subsection E as well.[245] Additionally, Representative Gabbard suggests adding an

[235] *See* Josh Zeman, "*A Slender Reed Upon Which to Rely": Amending the Espionage Act to Protect Whistleblowers*, 61 WAYNE L. REV. 149, 165 (2015).
[236] *See* Protect Brave Whistleblowers Act of 2020, H.R. 8452, 116th Cong. §799B (2020).
[237] *See* National Association for Legal Support, *supra* note 182.
[238] *See id.*
[239] *See generally* Protect Brave Whistleblowers Act of 2020, H.R. 8452, 116th Cong. (2020).
[240] *See id.* at § 2(a)(1).
[241] *See id.*
[242] *See id.* at § 2(a)(2) (2020).
[243] *See id.* at § 2(a)(3) (2020).
[244] *See* Protect Brave Whistleblowers Act of 2020, H.R. 8452, 116th Cong. § 2(a)(4) (2020).
[245] *See id.* at § 2(a)(5) (2020).

affirmative defense.[246] The proposed language suggests the affirmative defense is for either § 793 or § 798 when the defendant "engaged in the prohibited conduct for the purpose of disclosing to the public (1) any violation of any law, rule, or regulation; or (2) gross mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety."[247] The proposed affirmative defense includes the exact definition of a whistleblower.[248]

While Gabbard's now-abandoned bill proposed many change to ensure that whistleblowers who leak information to aid the public's knowledge are protected, it did not go goes far enough in some respects and went too far in others. Representative Gabbard wanted to add an affirmative defense that covered several motives.[249] This solution went too far. The affirmative defense should not, as hers did, cover "gross mismanagement, a gross waste of funds, or a substantial and specific danger to public health or safety."[250] Furthermore, the "violation of any law, rule, or regulation"[251] is too broad because some violations of existing law could be easily avoided by following the proper channels of the intelligence community whistleblower laws. That is to say, some disclosures are not illegal, and in fact protected, when made to the right person.[252] This could be as simple as talking to one's boss or making an official, formal submission through an IG hotline.[253] The affirmative defense should only cover something that affects our entire society, such as the Snowden NSA disclosures, to balance national security and state secrets with an informed democracy.[254] When information concerning a major societal issue is leaked, that leak allows citizens (whom our government is obliged to

[246] *See id.* at § 799B (2020).
[247] *See id.*
[248] *See* National Whistleblower Center, *supra* note 28.
[249] *See* Protect Brave Whistleblowers Act of 2020, H.R. 8452, 116th Cong. § 799B (2020).
[250] *See id.* at § 799B(2) (2020).
[251] *See id.* at §799B(1) (2020).
[252] *See* Office of the Dir. of Nat'l Intelligence, *How Do I Report?,* https://www.dni.gov/ICIG-Whistleblower/process-how.html (last visited Jan. 6, 2023).
[253] *See id.*
[254] *See* DYCUS ET AL., *supra* note 22.

protect) a chance to participate in democracy and give informed criticism.[255]

One may think that more legislation is the best way to address the lack of protection for those who leak information. While such an approach is good in theory, the reality is that there are already many statutory protections in place. The intelligence community has three sources of protection against whistleblowers who are retaliated against by their employers.[256] These come from the ICWPA, PPD-19, and Title VI.[257] These statutes are largely ignored when an individual decides to leak sensitive information.[258] Adding additional legislation is not the most feasible option when there are three whistleblower frameworks already in place. Instead, one solution would be combining them to render them less convoluted, so that potential whistleblowers may more easily decipher who and what is protected. That would not be a feasible solution to this problem, mainly because it has partially already been done. For instance, the PPD-19 expanded protections that came from ICWPA and Title VI increased protections from PPD-19.[259]

Overall, amending the Espionage Act to include a specific definition of "national defense," switching culpability to make it a specific intent crime, and adding an affirmative defense is likely the most politically palatable solution, because representatives from both major parties have endorsed similar propositions.[260] Moreover, such a solution could somewhat ameliorate the persistent concerns about abuse.[261]

---

[255] *See* United States v. Morison, 844 F.2d 1057, 1081 (4th Cir. 1988) (Wilkinson, J., concurring) (illustrating that courts believe there should be some limit to what is a state secret as opposed to information the government wishes citizens could not criticize).

[256] *See* CONG. RSCH. SERV., R43765, INTEL. WHISTLEBLOWER PROTECTIONS: IN BRIEF, 1 (2014).

[257] *See id.*

[258] *See* Pozen, *supra* note 29, at 527.

[259] *See* CONG. RSCH. SERV., R43765, INTEL. WHISTLEBLOWER PROTECTIONS: IN BRIEF, 1 (2014).

[260] *See* Kim, *supra* note 13; *see also* Protect Brave Whistleblowers Act of 2020, H.R. 8452, 116th Cong. (2020).

[261] *See* Kim, *supra* note 13.

CONCLUSION

The current Espionage Act is outdated, unconstitutionally vague, and can lead to serious policy discrepancies. Section 793 of the Act lacks consistency at its core. To address these problems and inconsistencies, the Espionage Act must be amended to include a narrowly tailored definition of "national defense" and what exactly is "related to" national defense. Additionally, the varying culpability requirements in the act should be changed to incorporate a specific intent element. Furthermore, an affirmative defense should be available for specific individuals. Congress has a duty to amend the Espionage Act of 1917 to ensure the due process rights of our citizens are upheld. If we are to uphold our nation's values, we need a better, and clearer, policy approach that consciously balances the needs of a democracy to know about the actions of its government, and the needs of a nation to protect its most sensitive and potentially dangerous secrets.