NOTES

PLAYING THE SAME GAME: WHY PROSECUTING ROBERT HANSSEN REQUIRES PROSECUTING EDWARD SNOWDEN

Becca Ebert*

ABSTRACT

There is often a stark divide in the public's discussion of the legal and moral culpability of spies and leakers. In common parlance, spies are duplicitous individuals who are sent to a country solely to obtain secrets or who betray their own country to divulge secrets to a foreign adversary, whereas leakers are principled individuals who assume great personal risk to publicly uncover government wrongdoing. Spies operate in the realm of foreign relations, prompting discussions of international law, while leakers work domestically, prompting analysis of government overreach and First Amendment protections. However, a legal and operational analysis of spies and leakers indicates that their actions are not as different as public discourse suggests.

This Note seeks to place spies and leakers within the same legal framework. By exploring the inadequacy of international law to regulate the collection and disclosure of government secrets, this Note centers on the Espionage Act's criminal prohibitions of the unauthorized access, disclosure, and receipt of sensitive information. Exploring the contours of the Espionage Act's application to spying and leaking requires understanding intelligence gathering operations and appreciating the harms resulting from the disclosure of sensitive information, whether from a spy or a leaker. This Note then argues that common calls to reform the Espionage Act—from asserting absolute First Amendment protection to exploring a defendant's subjective intent—are untenable in practice and undermine the goals of the Act: to protect against harms to national security by deterring the unauthorized disclosure of sensitive information. Instead, this Note argues that the current operation of the Espionage Act strikes a fair balance between protecting national security and upholding the fundamental values of this country. This Note calls for prosecutorial decisions that promote the Act's deterrent effect and improve public perceptions of the Act's legitimacy. Finally, this Note hopes to spark the simultaneous appreciation for the complex decisions necessary to keep this country secure and gratitude for the values and principles that make this country worth securing.

---

* J.D. from Georgetown University Law Center (2024); M.A. in Security Studies from Georgetown University (2024); B.S. in Mathematics from University of Puget Sound (2016); B.A. in Politics and Government from University of Puget Sound (2016). Sincere thanks to Professor Mary DeRosa for her feedback on this paper and her experienced guidance in the space of national security lawyering. Many thanks to the entire staff of ACLR for their thoughtful and detailed review.

INTRODUCTION

June 2023 was a notable month in the world of espionage. On June 5, 2023, Robert Hanssen, a former Federal Bureau of Investigation (FBI) agent convicted of spying for Moscow, died in his prison cell.[1] The very next day marked the ten-year anniversary of the first media story revealing classified information that Edward Snowden removed from the National Security Agency (NSA).[2] Hanssen's and Snowden's actions are strikingly similar: accessing and disseminating

1. Peter Baker, *Robert Hanssen, F.B.I. Agent Exposed as Spy for Moscow, Dies at 79*, N.Y. TIMES (June 5, 2023), https://www.nytimes.com/2023/06/05/us/robert-hanssen-spy-dead.html.

2. David Smith, *What's Really Changed 10 Years After the Snowden Revelations?*, GUARDIAN (June 7, 2023), https://www.theguardian.com/us-news/2023/jun/07/edward-snowden-10-years-surveillance-revelations.

numerous highly classified documents without authorization. Indeed, both were indicted under the Espionage Act. Hanssen pled guilty to fifteen counts of espionage and was sentenced to life in prison.[3] Snowden was charged with violating two provisions of the Espionage Act[4] and is currently living in Russia to avoid prosecution.[5] Despite the similarity of their charged activities and the years since Hanssen's 2001 arrest and Snowden's 2013 disclosure, public opinion toward these individuals differs drastically—even irreconcilably. Hanssen is remembered as "the most damaging spy in bureau history,"[6] while Snowden, to many, "will go down in history as one of America's most consequential whistleblowers."[7]

These opposing reputations highlight how the recipient of classified materials influences public perception. Hanssen's disclosures to foreign agents exemplify "classic spying" whereas Snowden's disclosures to the media constitute "leaking."[8] Hanssen and Snowden represent extreme cases, yet recent indictments demonstrate the continued divergence in public opinion. Also in June 2023, then-former President Donald Trump and Massachusetts Air National Guardsman Jack Teixeira were separately indicted for disclosing classified information. On June 8, 2023, Trump was indicted under the Espionage Act[9] for retaining classified documents as a private citizen[10] and disclosing classified information to third parties, including an Australian businessman.[11] On June 15, 2023, Teixeira was indicted for

3. Baker, *supra* note 1.

4. Complaint, United States v. Snowden, No. 1:13-CR-265-(CMH) (E.D. Va. June 14, 2013).

5. Smith, *supra* note 2.

6. Baker, *supra* note 1.

7. Glenn Greenwald, Ewen MacAskill & Laura Poitras, *Edward Snowden: The Whistleblower Behind the NSA Surveillance Revelations*, GUARDIAN (June 11, 2013), https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance.

8. There are no standardized definitions for "spying" and "leaking." For ease, this Note uses "spy" to refer to "classic spying," often defined as the secret disclosure of classified information to foreign agents working against the spy's country, and "leaker" to refer to the unauthorized disclosure of classified information to the media. *See, e.g.*, Ursula Wilder, *The Psychology of Espionage and Leaking in the Digital Age*, 61 STUD. INTEL. 1, 2 (2017), https://www.cia.gov/resources/csi/static/Psych-of-Leaking-Espionage.pdf ("Spies engaged in espionage secretly deliver classified information to a party the spy understands is working directly against his or her own country . . . . Spies who leak make classified information publicly available without authorization, usually through contacts with media outlets or via the Internet."). However, the central argument of this Note is that such distinctions are arbitrary, and both spies and leakers are committing espionage.

9. Indictment at 28, United States v. Trump, No. 23-80101-CR, 2024 WL 3404555 (S.D. Fla. July 15, 2024). The U.S. District Court for the Southern District of Florida dismissed the case on grounds that the special prosecutor lacked proper authority. *Trump*, 2024 WL 3404555, at *46–47. The government initially appealed but eventually moved to dismiss the case after the November 2024 election. *See, e.g.*, Hugo Lowell, *Prosecutors Drop Election Interference and Documents Cases Against Trump*, GUARDIAN (Nov. 25, 2024), https://www.theguardian.com/us-news/2024/nov/25/trump-criminal-case-dismissed.

10. Alan Feuer, Maggie Haberman, William K. Rashbaum & Ben Protess, *Trump Is Charged in Classified Documents Inquiry*, N.Y. TIMES (Aug. 17, 2023), https://www.nytimes.com/live/2023/06/08/us/trump-indictment-documents#justice-department-charges-trump-in-documents-case; Max Matza, *If Trump Isn't a Spy, Why Is He Being Charged Under the Espionage Act?*, BBC (June 14, 2023), https://www.bbc.com/news/world-us-canada-65910903.

11. Alan Feuer, Ben Protess, Maggie Haberman & Jonathan Swan, *Trump Said To Have Revealed Nuclear Submarine Secrets to Australian Businessman*, N.Y. TIMES (Oct. 5, 2023), https://www.nytimes.com/2023/10/05/us/politics/trump-nuclear-submarine-classified-documents.html.

disclosing classified documents to social media sites including Twitter, Discord, and Telegram.[12] These two indictments further complicate any clear delineation between "classic spying" and "leaking." Despite the involvement of foreign nationals, Trump's supporters resolutely disclaim that he is a spy.[13] Teixeira's disclosures to social media chat groups question what qualifies as the "media" to warrant leaker status.[14] Cutting through the power of how public perceptions frame these actions requires a close exploration of the legal framework behind espionage.

Legal discussions of espionage generally track two distinct narratives: international spying or domestic leaking. In international relations, peacetime espionage operates within the international legal framework.[15] Foreign agents work at the direction of one state to obtain secret information about another state, i.e., "classic spying." Under this framework, individuals caught spying are subject to strict punishment under domestic legal regimes.[16] This spying includes foreigners operating abroad or citizens recruited to betray their home country. Public perception in the United States seems to hold that these foreign agents deserve prosecution under the Espionage Act.[17] The second narrative emphasizes only domestic law. The unauthorized disclosure of classified information to the media, i.e., "leaking," is viewed as a solely domestic act operating under U.S. constitutional protections. To many in the United States, prosecuting leakers under the Espionage Act is an unconstitutional infringement on free speech and press.[18]

This Note argues that the distinction between these two narratives is manufactured, inaccurate, and harmful. There exists no principled legal distinction between "classic spying" and "leaking." Moreover, protecting against espionage's damage to national security requires treating these cases the same. In short, deterring a future Robert Hanssen requires prosecuting an Edward Snowden.

Part I describes the international legal framework addressing espionage, finding that deterring and punishing acts of espionage must be accomplished via domestic law. Part II outlines the U.S. domestic regime to prosecute acts of espionage by citing the Espionage Act's provisions and its operation in criminal prosecutions as it

---

12. Press Release, U.S. Dep't of Just., Air National Guardsman Indicted for Unlawful Disclosure of Classified National Defense Information (June 15, 2023), https://www.justice.gov/opa/pr/air-national-guardsman-indicted-unlawful-disclosure-classified-national-defense-information; Juliana Kim & Jenna McLaughlin, *What We Know About Jack Teixeira, The Suspected Leaker of Pentagon Documents*, NPR (Apr. 14, 2023), https://www.npr.org/2023/04/14/1169952771/jack-teixeira-background-pentagon-document-leak.

13. Matza, *supra* note 10 (quoting U.S. Sen. Lindsey Graham: "You may hate his guts, but he is not a spy; he did not commit espionage").

14. *See* Charlie Savage, *Teixeira's Case Is Unusual Even in the Small World of Leak Cases*, N.Y. TIMES (Apr. 14, 2023), https://www.nytimes.com/2023/04/14/us/politics/jack-teixeira-leaked-documents-case.html.

15. *See, e.g.*, Kathryn Jane Browne, *The Paradox of Peacetime Espionage in International Law: From State Practice to First Principles*, 23 AUSTL. INT'L L.J. 109, 110 (2017).

16. *See id.* at 111.

17. Extensive research by the author failed to uncover substantial criticism of the Espionage Act's application to foreign agents accused of spying against the United States.

18. *See, e.g.*, Heidi Kitrosser & David Schulz, *A House Built on Sand: The Constitutional Infirmity of Espionage Act Prosecutions for Leaking to the Press*, 19 FIRST AMEND. L. REV. 153, 153–56 (2021).

relates to spies and leakers. Part III discusses potential avenues to distinguish "classic spying" from "leaking" under the Espionage Act, concluding that any such distinction is practically unworkable and causes deleterious consequences. Part IV notes that the Espionage Act currently balances the competing interests of national security and constitutional protections, suggesting reforms to improve the coherence and legitimacy of the Espionage Act's application to spies and leakers.

I. THE INCONSEQUENCE OF INTERNATIONAL LAW IN REGULATING ESPIONAGE

On May 1, 1960, Francis Gary Powers' U-2 plane was shot down over the U.S.S.R.[19] Initially claiming it to be a NASA weather plane, President Dwight D. Eisenhower later admitted to the U-2's espionage, noting that this activity is a "distasteful but vital necessity."[20] Following the Soviet's indignant response, the United States touted a list of the Soviet's own espionage activities.[21] The U-2 incident is rare, as states generally do not acknowledge engaging in espionage,[22] but the incident also exemplifies espionage's double standard: if beneficial to a state, espionage is a vital tool of statecraft; if detrimental, it is an affront to diplomatic relations.[23] This duality complicates the legality of espionage in international law. This Part of the Note traces the main arguments of this legal debate to no avail: there is no conclusive resolution to peacetime espionage's legality where each side employs the same principles to argue opposite conclusions. Regardless of espionage's legality or illegality, however, this Part concludes that the legal status of peacetime espionage is irrelevant to the practice of espionage. After first tracing the treatment of espionage in international treaties and customary international law (CIL), this Part discusses examples of espionage's vital role in facilitating diplomacy, suggesting that international law will not regulate the practice of espionage. Thus, domestic criminal laws offer the only legal deterrent to espionage.

A. Espionage in International Law

Considering the widespread practice of espionage, international law plays a surprisingly small role in regulating espionage activities. Many note that, outside the laws of war, international law is silent regarding espionage.[24] That is, peacetime espionage is a practice neither allowed nor outlawed. However, this conclusion

19. Evan Andrews, *When a US Spy Plane Was Shot Down Over the USSR*, HIST. (Feb. 3, 2023), https://www.history.com/news/u-2-spy-plane-incident-ussr.

20. *Id.*

21. *Id.*

22. *See* Richard A. Falk, *Foreword* to QUINCY WRIGHT, JULIUS STONE, RICHARD A. FALK & ROLAND J. STANGER, ESSAYS ON ESPIONAGE AND INTERNATIONAL LAW, at vii (Roland J. Stanger ed., 1962).

23. *See* A. John Radsan, *The Unresolved Equation of Espionage and International Law*, 28 MICH. J. INT'L L. 595, 608–09 (2007).

24. *See* Iñaki Navarrete & Russell Buchan, *Out of the Legal Wilderness: Peacetime Espionage, International Law and the Existence of Customary Exceptions*, 51 CORNELL INT'L L.J. 897, 899 (2019).

generates significant debate.[25] Others argue that there is no silence: international law clearly covers peacetime espionage, but they still disagree whether it is illegal or legal.[26]

International law expressly recognizes espionage only during war. The laws of armed conflict define a spy and establish minimal requirements for spies' treatment.[27] The Hague and Geneva Regulations determine that captured spies are not prisoners of war[28] and can only be punished after a trial.[29] Further, a spy who returns home from belligerent territory is immune from any previous acts of spying if recaptured by the enemy.[30] These provisions of the laws of war suggest an acceptance of the role of spies in the conduct of war yet sanction the ultimate penalty for captured spies.[31]

Despite this clear recognition of spies during wartime, international law does not expressly acknowledge peacetime espionage.[32] There is no body of international law, treaty, or judicial ruling that explicitly discusses the permissibility of peacetime espionage.[33] The *Lotus* principle gives credence to this silence. Originating from the Permanent Court of International Justice's 1927 opinion regarding the collision of the French ship *S.S. Lotus* with a Turkish ship, the *Lotus* principle asserts that state sovereignty is a fundamental principle of international relations and concludes that a state can act unless an established international rule

---

25. François Dubuisson & Agatha Verdebout, *Espionage in International Law*, OXFORD BIBLIOGRAPHIES (Sept. 25, 2018), https://www.oxfordbibliographies.com/display/document/obo-9780199796953/obo-9780199796953-0173.xml.

26. Browne, *supra* note 15, at 112–15.

27. The 1907 Hague Convention defines a spy as someone who, "acting clandestinely or on false pretences . . . obtains or endeavours to obtain information in the zone of operations of a belligerent, with the intention of communicating it to the hostile party." Convention (IV) Respecting the Laws and Customs of War on Land and Its Annex: Regulations Concerning the Laws and Customs of War on Land art. 29, Oct. 18, 1907, 36 Stat. 2277 [hereinafter Hague Convention IV], https://ihl-databases.icrc.org/assets/treaties/195-IHL-19-EN.pdf. Key to this definition is the clandestine or false nature of activity. A soldier in uniform performing the same actions is not considered a spy. *Id.*

28. *See* Protocol Additional to the Geneva Conventions of 12 Aug. 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I) art. 46, 8 June, 1977, 1125 U.N.T.S. 3 [hereinafter Geneva Protocol I], https://ihl-databases.icrc.org/assets/treaties/470-AP-I-EN.pdf.

29. *See* Hague Convention IV, *supra* note 27, art. 30.

30. *See id.* art. 31; Geneva Protocol I, *supra* note 28, art. 46.

31. *See* Browne, *supra* note 15, at 111.

32. Some argue the comparison of international law's treatment of wartime and peacetime espionage suggests legality. Citing the principle of *expressio unius,* some argue peacetime espionage is unlawful because, unlike wartime espionage, it is not expressly permitted. Others similarly cite *expressio unius* for the opposite conclusion: espionage is generally lawful and wartime espionage provisions are the only restrictions to the general practice. *See* Jared Beim, *Enforcing a Prohibition on International Espionage*, 18 CHI. J. INT'L L. 647, 653–54 (2018).

33. The International Court of Justice (ICJ) avoids ruling on the legality of espionage. The ICJ rejected arguments that alleged U.S. espionage conducted from the U.S. embassy in Tehran justified the subsequent taking of hostages. *See* United States Diplomatic and Consular Staff in Tehran (U.S. v. Iran), Judgment, 1980 I.C.J. 1, ¶¶ 80–88 (May 24). Additionally, the ICJ never ruled whether Australia using listening devices during negotiations with Timor-Leste voided the resulting treaty because Timor-Leste dropped its claim. *See* Questions Relating to the Seizure and Detention of Certain Documents and Data (Timor-Leste v. Australia), Order of Discontinuance, 2015 I.C.J. 572, 574 (June 11); Browne, *supra* note 15, at 109.

prohibits the conduct.[34] Proponents of espionage's legality cite *Lotus* to conclude that the activity is permissible absent any rule restricting the practice.[35] Proponents of espionage's illegality cite *Lotus* to emphasize espionage's violation of fundamental legal principles,[36] including sovereignty,[37] nonintervention,[38] government function,[39] and sovereign equality.[40] Either way, there exists no express permission or prohibition of peacetime espionage.

Although treaties contain no explicit references to espionage, treaties often tacitly acknowledge the practice and provide procedural remedies. Treaties regulating the conduct of diplomatic and consular officials[41] protect diplomacy from espionage by shielding diplomatic operations from outside intrusion.[42] These treaties also prohibit espionage by diplomats[43] by requiring diplomatic staff to respect the laws of their host state, refrain from interfering in the host state's internal affairs, and avoid using the premises "in any manner incompatible with the functions of the mission."[44] However, the privileges of diplomatic and consular immunity ensure officials accused of espionage are not prosecuted but are instead declared *persona non grata* and recalled to their home state.[45] Such relaxed punishments suggest a simultaneous prohibition of and acquiescence to espionage.

CIL similarly lacks conclusion on espionage's legality. Akin to international common law, CIL is the collection of practices governing state conduct outside of formal treaties. CIL requires widespread, longstanding state practice performed

---

34. *See* S.S. Lotus (Fr. v. Turk.), 1927 P.C.I.J. (ser. A), No. 10, at 18–20 (Sept. 7); Patrick C. R. Terry, *"The Riddle of the Sands" – Peacetime Espionage and Public International Law*, 51 GEO. J. INT'L L. 377, 381 (2020).

35. *See S.S. Lotus*, 1927 P.C.I.J. (ser. A) at 18–20; Terry, *supra* note 34, at 381.

36. *See* Browne, *supra* note 15, at 118–20.

37. *See* Terry, *supra* note 34, at 390 (critiquing this argument); Quincy Wright, *Espionage and the Doctrine of Non-Intervention in Internal Affairs, in* WRIGHT ET AL., *supra* note 22, at 3, 12.

38. *See* Wright, *supra* note 37, at 13.

39. *See* Terry, *supra* note 34, at 395–97.

40. *See* Browne, *supra* note 15, at 120–21.

41. The Vienna Convention on Diplomatic Relations (VCDR) and the Vienna Convention on Consular Relations (VCCR) govern the operation of states' diplomatic and consular activities, respectively. *See generally* Vienna Convention on Diplomatic Relations, Apr. 18, 1961, 500 U.N.T.S. 95, https://legal.un.org/ilc/texts/instruments/english/conventions/9_1_1961.pdf [hereinafter VCDR]; Vienna Convention on Consular Relations, Apr. 24, 1963, 596 U.N.T.S. 261, https://legal.un.org/ilc/texts/instruments/english/conventions/9_2_1963.pdf [hereinafter VCCR].

42. The VCDR and VCCR contain multiple provisions asserting the inviolability of diplomatic and consular functions. *See* VCDR, *supra* note 41, arts. 22, 24, 27; VCCR, *supra* note 41, arts. 31 (buildings and premises), 33 (documents), 35 (official correspondence).

43. States may send spies with "official cover" who are diplomatic or consular staff and are afforded diplomatic immunity. States may also send spies with "non-official cover," known as NOCs or illegals. Because they do not enjoy diplomatic immunity, NOCs are subject to the domestic laws of the capturing state. Their activities are also disavowed where a state typically does not admit to sending a spy. *See* Radsan, *supra* note 23, at 620–22.

44. VCDR, *supra* note 41, art. 41; *see also* VCCR, *supra* note 41, art. 55. Respecting internal laws encompasses espionage where there is a near-universal prohibition of espionage in states' domestic laws. *See* Navarrete & Buchan, *supra* note 24, at 911.

45. *See* Simon Chesterman, *The Spy Who Came in from the Cold War,* 27 MICH. J. INT'L L. 1071, 1088–89 (2006).

from a sense of legal obligation (*opinio juris*), not merely habit, ease, or policy.[46] Espionage is certainly a widespread and longstanding practice,[47] but *opinio juris* complicates the creation of a customary rule because of the general practice of state silence following accusations of espionage. With the notable exception of U.S. admissions following the U-2 incident[48] and revelations of NSA surveillance,[49] states maintain conspicuous silence or denial of spying accusations.[50] No state publicly denounces espionage as illegal because that determination would apply to the state's own espionage.[51] Furthermore, no state claims a right to spy[52] because such a right would belong to every state, undermining the ability to punish adversarial spies. Thus, states express disapproval through diplomacy. States frequently engage in mutual diplomatic expulsions[53] or prisoner exchanges of accused spies.[54] Despite the ubiquity of these responses, the practice fails to communicate a legal obligation necessary to establish CIL.[55] Treaties and CIL do not definitively conclude the legality of peacetime espionage, yet this absence of clarity is immaterial considering the benefits of espionage.

B. A Practical Approach

Peacetime espionage is an essential tool in foreign affairs that states are unlikely to voluntarily relinquish. Arguing over espionage's legality or proposing the

---

46. *See* Int'l Law Comm'n, Rep. on the Work of Its Seventieth Session, U.N. Doc. A/73/10, at 124 (2018) ("To determine the existence and content of a rule of customary international law, it is necessary to ascertain whether there is a general practice that is accepted as law (*opinio juris*).").

47. *See* Navarrete & Buchan, *supra* note 24, at 947.

48. *See* Wright, *supra* note 37, at 14.

49. *See* Navarrete & Buchan, *supra* note 24, at 941–42.

50. *See id.* at 935 ("States have consistently refused to acknowledge their participation in espionage activities."); Wright, *supra* note 37, at 13–14.

51. *See* Radsan, *supra* note 23, at 619. Radsan observes:

> [T]he United States could make it a crime for its citizens to steal military, diplomatic, and intelligence secrets from other countries. But the reward for such self-righteousness would be mockery and disbelief. Other states would not then preclude their intelligence services from stealing secrets from foreigners and foreign governments. Even if they took that step, they would not enforce the preclusion.

Id.

52. *See* THIBAULT MOULIN, CYBER-ESPIONAGE IN INTERNATIONAL LAW: SILENCE SPEAKS 269 (2023).

53. Following Hanssen's arrest, President George W. Bush expelled fifty Russian diplomats. Russian President Vladimir Putin then responded by expelling fifty American diplomats. Although it is evident this reciprocal response resulted from Hanssen's uncovered espionage, there is no indication this diplomatic punishment reflected the international illegality of Russia's actions in cultivating Hanssen's espionage. *See* Baker, *supra* note 1.

54. August 2024 saw the largest prisoner swap between the U.S. and Russia since the Cold War and included the exchange of accused spies. It is important to note Russian allegations of espionage, especially toward journalists, may not be well-founded and instead are aimed to suppress international criticism of the government. *See* Anton Troianovski & Mark Mazzetti, *Major Inmate Swap Frees Dissidents and U.S. Journalists from Russian Prisons*, N.Y. TIMES (Aug. 1, 2024), https://www.nytimes.com/2024/08/01/world/europe/russia-gershkovich-prisoner-swap.html.

55. *See* Navarrete & Buchan, *supra* note 24, at 928.

adoption of a treaty defining the contours of the practice are largely theoretical exercises. Instead, embracing the functional, yet paradoxical, status of espionage enables a practical approach to foreign relations.

Espionage facilitates international cooperation. Without intelligence to verify a state's expressed intent or monitor treaty obligations, states may be less willing to trust other states, thus diminishing international cooperation.[56] International arms control agreements demonstrate the utility of espionage and intelligence gathering to international cooperation.[57] During the Cold War, U.S.-U.S.S.R. arms control negotiations stalled when determining how to verify compliance.[58] However, both states possessed extensive surveillance capabilities, which was expressly written into the Anti-Ballistic Missile Treaty and SALT I Agreement, where each state would employ "national technical means of verification" to monitor compliance.[59]

In addition to facilitating cooperation, espionage is essential for self-defense, allowing states to monitor potential risks before they become imminent.[60] During the U-2 incident, for example, the Secretary of State expressly argued the U.S. government "would be derelict to its responsibility not only to the American people but to free peoples everywhere if it did not, in the absence of Soviet cooperation, take such measures as are possible unilaterally to lessen and to overcome this danger of surprise attack."[61] This responsibility to monitor allowed the United States to detect the construction of Soviet missile sites in Cuba in October 1962.[62] The ability to discover these missiles at installation, rather than once they were launched, allowed President John F. Kennedy the time to de-escalate a potential nuclear confrontation during the Cuban Missile Crisis.[63] In practice, espionage facilitates international cooperation.[64]

Whether international legal principles sanction or prohibit espionage is immaterial to the practice of espionage. States are unlikely to alter their behavior even if international law scholars reach consensus on espionage's legal status. Furthermore, the benefits of espionage to states' security precludes efforts to enact treaties restricting espionage.[65] Espionage's role in state cooperation suggests it would be unwise to do

---

56. *See* Christopher Baker, *Tolerance of International Espionage: A Functional Approach*, 19 AM. U. INT'L L. REV. 1091, 1104–06 (2004).

57. *See generally* Roland J. Stanger, *Espionage and Arms Control*, *in* WRIGHT ET AL., *supra* note 22, at 83.

58. *See* Chesterman, *supra* note 45, at 1090–91 (quoting Treaty on the Limitation of Anti-Ballistic Missile Systems, U.S.-U.S.S.R., art. XII, May 26, 1972, 23 U.S.T. 3435; Interim Agreement on Certain Measures With Respect to the Limitation of Strategic Arms, U.S.-U.S.S.R., art. V., May 26, 1972, 23 U.S.T. 3463).

59. *See id.*

60. *See* Baker, *supra* note 56, at 1096; *see also* Terry, *supra* note 34, at 382–83.

61. Press Release, U.S. Dep't of State, Statement by the Secretary of State (May 9, 1960), https://www.eisenhowerlibrary.gov/sites/default/files/research/online-documents/u2-incident/5-9-60-no254.pdf.

62. *See* Baker, *supra* note 56, at 1096–97.

63. *See id.*

64. *See id.* at 1097.

65. The few attempts to secure agreements limiting espionage were unsuccessful. *See* MOULIN, *supra* note 52, at 279–280 (noting four proposals to limit espionage between states that were unsuccessful: In 1979, Vietnam requested China to agree not to spy; in 2013, Indonesia requested an agreement from Australia; in 2013,

so.[66] Instead, recognizing that international law is unlikely to ever clearly regulate espionage allows states to focus on regulating espionage where it truly matters: domestic law.

C. Domestic Law Fills the Gap

While it is true that states often fall silent following accusations of espionage, the practice of espionage regularly occurs, leading one international law scholar to conclude: "Intelligence is less a lacuna in the legal order than it is the elephant in the room."[67] The United States need only name Robert Hanssen, Aldrich Ames,[68] or the Russian spy ring busted in 2010[69] to illuminate the immense harm that espionage poses to national security. Yet, Russia need only cite those same names and the information they provided to illuminate the immense benefit espionage poses to national security. This duality defines the essential feature of espionage: spies play the same game for different sides.[70] In fact, Hanssen was identified only after a former Russian intelligence officer provided the United States with information in exchange for $7 million.[71] Whether it is obtaining crucial information from adversaries or rooting out spies within government ranks, espionage promises substantial national security advantages. The benefits of this game are worth the risks.

Although espionage is not internationally outlawed, it is almost universally outlawed via states' domestic laws.[72] International law and diplomatic relations are

---

Luxembourg proposed an EU agreement; in 2014, Germany demanded a "no-spy agreement" from the U.S). U.S. officials expressly admit the undesirability of such agreements. Admiral Vern Clark, commenting on a treaty, said, "I want to be on record saying that we would never recommend a treaty that would . . . restrict our intelligence activities around the world, because we know that those kinds of freedoms are essential to what we have to do to be successful in our mission." *Id*.

66. *See, e.g.*, *Transcript: Obama's Speech on N.S.A. Phone Surveillance*, N.Y. TIMES (Jan. 17, 2014), https://www.nytimes.com/2014/01/18/us/politics/obamas-speech-on-nsa-phone-surveillance.html. U.S. President Barack Obama stated:

> Meanwhile, a number of countries, including some who have loudly criticized the NSA, privately acknowledge that America has special responsibilities as the world's only superpower; that our intelligence capabilities are critical to meeting these responsibilities, and that they themselves have relied on the information we obtain to protect their own people.

Id.; MOULIN, *supra* note 52, at 275 (quoting former French Ministry of Foreign Affairs official Bernard Kouchner who noted France was "shocked by the scale of eavesdropping. But to be honest, we listen to them too. Everybody is listening to everybody. We simply do not have the same means as the United States, and we are jealous of it").

67. *See* Chesterman, *supra* note 45, at 1072.

68. Aldrich Ames was an American CIA officer who spied for the U.S.S.R. and then Russia from 1985 until his arrest in 1994. The secrets he divulged included the identities of human sources working in the Soviet Bloc. Some were executed as a result. *See Aldrich Ames*, FED. BUREAU OF INVESTIGATION, https://www.fbi.gov/history/famous-cases/aldrich-ames (last visited Oct. 14, 2024).

69. *See Suspected Russian Spies Charged in US*, BBC (June 29, 2010), https://www.bbc.com/news/10442223.

70. *See* Chesterman, *supra* note 45, at 1099; Radsan, *supra* note 23, at 608 ("If an American officer . . . goes over to the other side, we call him a traitor. We prosecute him to the fullest extent possible. But if someone from the other side . . . comes to our side, we admire him.").

71. *See* Baker, *supra* note 1.

72. *See supra* note 44.

ineffective at deterring and punishing acts of espionage. A state calling foul for espionage invites reciprocal protest toward that state's own spies.[73] When foreigners who have diplomatic status are caught spying, they are recalled to their home state unscathed.[74] Thus, catching a foreign spy without this diplomatic cover or a country's own citizen serving as a mole to benefit another state are the only true instances where espionage is punished.[75] The sending state often disavows any espionage activity—leaving the individual subject to that state's domestic laws.[76] Nearly all states have domestic laws criminalizing espionage activities.[77] Thus, domestic criminal regimes offer the only avenue to punish and deter espionage on the international stage.

II. THE REQUIREMENTS OF DOMESTIC LAW TO PUNISH AND DETER ESPIONAGE

Where diplomatic rebuke and expulsion are insufficient deterrents, domestic laws criminalizing espionage are required to deter and punish adversarial spies. Under U.S. law, the Espionage Act ("the Act") is the main vehicle to punish espionage conducted to the United States' detriment. However, the Espionage Act is often condemned as "unconstitutional,"[78] "misguided,"[79] or even "one of the scariest statutes around."[80] To understand—and dispel—these criticisms, this Part examines the history, terms, and use of the Espionage Act since its passage. This Part first discusses the Act's passage and early targeting of political rivals. Although critics assert the Act continues to target political rivals by prosecuting leakers, prosecutions of leakers remain relatively rare. Then, examining the Act's language conveys the breadth of activities covered under this Act. Other laws prohibit similar activities but are narrower in scope and thus have a weaker deterrent effect than the Espionage Act. To conclude, this Part discusses how unique aspects of Espionage Act prosecutions, especially the need to avoid further disclosure of

73. Strident denunciations of espionage are undermined by the "clean hands" principle where states allegations of violations shall not be given credence when they are guilty of violations themselves. *See* Patrick C.R. Terry, *"Don't Do as I Do" — The US Response to Russian and Chinese Cyber Espionage and Public International Law*, 19 GERMAN L.J. 613, 624 (2018).

74. *See* Radsan, *supra* note 23, at 621 (noting that expelled diplomats will not be criminally punished for their activities, just reprimanded for "professional incompetence").

75. Extradition treaties are often ineffective for alleged espionage. Espionage is often considered a political offense, which is expressly excluded from extradition. As such, spies caught outside the harmed state are unlikely to be returned to face prosecution. Spies apprehended in the harmed state are subject to standard criminal procedures. *See* Monika B. Krizek, *The Protective Principle of Extraterritorial Jurisdiction: A Brief History and an Application of the Principle to Espionage as an Illustration of Current United States Practice*, 6 B.U. INT'L L.J. 337, 357–58 (1988); Radsan, *supra* note 23, at 609 ("For a spy, sometimes one international flight makes all the difference in the world.").

76. *See* Radsan, *supra* note 23, at 622; *see also* Wright, *supra* note 37, at 13–14.

77. *See* MOULIN, *supra* note 52, at 244–50 (surveying countries' national laws criminalizing espionage).

78. Recent Case, United States v. Rosen*, 445 F. Supp. 2d 602 (E.D. Va. 2006)*, 120 HARV. L. REV. 821, 821 (2007).

79. Kitrosser & Schulz, *supra* note 18, at 154.

80. Stephen I. Vladeck, *Inchoate Liability and the Espionage Act: The Statutory Framework and the Freedom of the Press*, 1 HARV. L. & POL'Y REV. 219, 223 (2007) (quoting SUSAN BUCKLEY, REPORTING ON THE WAR ON TERROR: THE ESPIONAGE ACT AND OTHER SCARY STATUTES 9 (2d ed. 2006)).

sensitive information, hinders the government's ability to explain and legitimize its prosecutions.

A. History and Use of the Espionage Act

Controversy has surrounded the Espionage Act since its inception. The Espionage Act was originally passed in 1917 to protect the military effort during World War I.[81] By its text, the Act protected the disclosure of information intended to impair the U.S. war effort or aid the enemy.[82] The Act quickly exceeded purely military objectives. Passage of the 1918 Sedition Act amended the law to punish those who "willfully utter, print, write, or publish any disloyal, profane, scurrilous, or abusive language" about the form of the U.S. government, the Constitution, or the military.[83] Critics of the war were quickly charged for any "disloyal utterances."[84] These prosecutions demolished First Amendment protection of political speech and were generally considered baldly political prosecutions of President Woodrow Wilson's opponents.[85] Faced with public furor, President Wilson eventually commuted numerous sentences, President Warren Harding commuted even more, and President Calvin Coolidge freed the remaining prisoners convicted under the Acts.[86] The Sedition Act was repealed in 1921, but the Espionage Act remains today with only minor amendments passed in 1948 and 1950.[87]

Despite this tumultuous beginning, the Espionage Act is repeatedly used to prosecute spies. The Act applies to foreign agents operating in the United States and

---

81. *See* David Forte, *Righting a Wrong: Woodrow Wilson, Warren G. Harding, and the Espionage Act Prosecutions*, 68 CASE W. RES. L. REV. 1097, 1101–02 (2018).

82. *See* Espionage Act of 1917, Pub. L. No. 65-24, § 3, 40 Stat. 217, 219 (codified as amended at 18 U.S.C. § 2388). The original Act stated:

> Whoever, when the United States is at war, shall willfully make or convey false reports or false statements with intent to interfere with the operation or success of the military or naval forces of the United States or to promote the success of its enemies and whoever when the United states is at war, shall willfully cause or attempt to cause insubordination, disloyalty, mutiny, refusal of duty, in the military or naval forces of the United States, or shall willfully obstruct the recruiting or enlistment service of the United States, to the injury of the service or of the United States, shall be punished by a fine of not more than $10,000 or imprisonment for not more than twenty years, or both.

Id.

83. *See* Sedition Act of 1918, Pub. L. No. 65-150, 40 Stat. 553 (amending *id.*) (repealed 1921).

84. Forte, *supra* note 81, at 1121, 1124 (quoting 1918 ATT'Y GEN. ANN. REP. 7, 18).

85. *See id.* at 1125 (noting that President Wilson referred cases to the Attorney General); Jameel Jaffer, *The Espionage Act Has Been Abused—But Not in Trump's Case*, POLITICO (Aug. 17, 2022), https://www.politico.com/news/magazine/2022/08/17/the-espionage-act-has-a-dark-history-prosecuting-trump-would-be-legit-00052376.

86. *See* Forte, *supra* note 81, at 1150.

87. *See* Scott Bomboy, *The Espionage Act's Constitutional Legacy*, NAT'L CONST. CTR.: CONST. DAILY BLOG (Aug. 17, 2023), https://constitutioncenter.org/blog/the-espionage-acts-constitutional-legacy.

government employees divulging secrets to foreign agents.[88] A complete chronicle of all Espionage Act prosecutions is beyond the scope of this Note, yet the number of prosecutions demonstrates the Espionage Act's utility in punishing spies working against U.S. national security interests.

In contrast, the Act's application to leakers is recent and less frequent. The first application of the Act to disclosures to the media occurred in 1957. Army Colonel Jack Nickerson was prosecuted by court martial for disclosing information about a missile program to the press.[89] The government dropped the Espionage Act charge, and Nickerson pled guilty for violating military regulations.[90] The second prosecution was of Daniel Ellsberg for disclosing the Pentagon Papers.[91] The case ended in mistrial due to prosecutorial misconduct.[92] The Espionage Act's first conviction for a leak was not until 1988, over sixty years after its passage. Samuel Morison was convicted of disclosing a classified photograph of a Soviet carrier to a British defense magazine.[93] Morison was later pardoned.[94] Following Morison's prosecution, the next prosecution was in 2005, targeting Lawrence Franklin for disclosing information to an Israeli diplomat and lobbying group.[95]

Between 1917–2009, these four cases were the only prosecutions of leakers.[96] Then, the Obama Administration aggressively prosecuted leakers under the Act, pursuing cases against eight leakers including the high-profile prosecution of Chelsea Manning and the indictment of Edward Snowden.[97] The Trump Administration followed suit, indicting eight leakers and investigating many more.[98] The Biden Administration prosecuted Jack Teixeira for his disclosures on social media, though some commentators suggest Teixeira is not a "leaker."[99]

---

88. *See, e.g.*, Press Release, U.S. Dep't of Just., U.S. Citizen and Four Chinese Intelligence Officers Charged with Spying on Prominent Dissidents, Human Rights Leaders and Pro-Democracy Activists (May 18, 2022), https://www.justice.gov/opa/pr/us-citizen-and-four-chinese-intelligence-officers-charged-spying-prominent-dissidents-human; Press Release, U.S. Dep't of Just., Two U.S. Navy Servicemembers Arrested for Transmitting Military Information to the People's Republic of China (Aug. 3, 2023), https://www.justice.gov/opa/pr/two-us-navy-servicemembers-arrested-transmitting-military-information-peoples-republic-china.

89. *See* Kitrosser & Schulz, *supra* note 18, at 173–74.

90. *See id.* at 174.

91. *See id.* at 175.

92. *See id.*

93. *See id.*

94. *See id.* at 176–77.

95. *See* STEPHEN MULLIGAN & JENNIFER ELSEA, CONG. RSCH. SERV., R41404, CRIMINAL PROHIBITIONS ON LEAKS AND OTHER DISCLOSURES OF CLASSIFIED DEFENSE INFORMATION 16 (2023).

96. See Kitrosser & Schulz, *supra* note 18, at 161.

97. Prosecutions of government officials under the Obama Administration include Shamai Leibowitz, Thomas Drake, Jeffrey Sterling, Stephen Jim-Woo Kim, Chelsea Manning, John Kiriakou, James Hitselberger, Donald Sachtleben, and Edward Snowden. *See* MULLIGAN & ELSEA, *supra* note 95, at 16–21.

98. Prosecutions under the Trump Administration include Julian Assange, Reality Winner, and Joshua Schulte. *See id.* at 22, 27–28; *see also* Kitrosser & Schulz, *supra* note 18, at 161–62.

99. In March 2024, Airman Jack Teixeira pled guilty to the "willful retention and transmission of national defense information" under the Espionage Act. Reporting has not treated Teixeira as a traditional leaker, often noting his intent to gain social clout on social media sites rather than a motivation to inform the public. *See, e.g.*, Maya Shwayder & Glenn Thrush, *Jack Teixeira Agrees to 16-Year Plea Deal in Document Leaks Case*,

Critics sound alarm at the increasing rate of such prosecutions whilst noting that the group of prosecuted leakers is still relatively small. Considering the ubiquity of leaks,[100] critics contend that the few prosecutions of low-level employees demonstrate selective enforcement reminiscent of WWI-era prosecutions.[101] The Act's historical backdrop gives credence to these claims that the prosecutions are examples of unprincipled political use of the Espionage Act. However, analyzing the legitimacy of these prosecutions requires understanding the express terms of the Act and its usage.

B. Current Provisions

The Espionage Act is the main statutory vehicle to punish spies and, more generally, the unauthorized collection or dissemination of information and materials impacting national security. The Espionage Act spans multiple sections of the criminal code, 18 U.S.C. §§ 792–799, but its main provisions are 18 U.S.C. §§ 793–794.[102] Both sections prohibit the transmittal of information and documents "relating to the national defense" that may "injur[e]" the United States or "advantage" a foreign nation.[103]

Section 794 broadly conforms to cases of "classic spying": § 794(a) prohibits the transmission of defense information to a foreign government or its agent,[104] § 794(b) specifies the conditions that apply during wartime,[105] and § 794(c)

N.Y. TIMES (Mar. 4, 2024), https://www.nytimes.com/2024/03/04/us/politics/jack-teixeira-guilty-classified-documents.html.

100. One survey indicated forty-two percent of government officials had leaked classified information to the press. *See* James Bruce, *Preventing Intelligence Leaks: Let's Start Over*, JUST SEC. (May 3, 2023), https://www.justsecurity.org/86404/preventing-intelligence-leaks-lets-start-over/.

101. *See, e.g.*, MULLIGAN & ELSEA, *supra* note 95, at 16 (observing that the DOJ came under criticism for the Morison prosecution "on the basis that such prosecutions are so rare as to amount to a selective prosecution"); RALPH ENGELMAN & CAREY SHENKMAN, A CENTURY OF REPRESSION: THE ESPIONAGE ACT AND FREEDOM OF THE PRESS 2 (2022) ("The playbook of Espionage Act prosecutions is tainted with the settling of political scores, character assassination, illegal break-ins, extrajudicial death threats, and prosecutorial misconduct.").

102. Sections 793 and 794 are most relevant to the discussion of classic spying and leakers and are the focus of this Note. The other sections prohibit harboring someone who violated §§ 793–794, 18 U.S.C. § 792; photographing and sketching military installations and equipment, *id.* § 795; using aircraft to document images of military installations and equipment, *id.* § 796; publishing any images of military installations or equipment, *id.* § 797; communicating or publishing signals intelligence, codes, or ciphers, *id.* § 798; and violating NASA's security regulations, *id.* § 799.

103. 18 U.S.C. §§ 793–794. Note the statute does not define "injury" or "advantage." Conceivably, any document that advantages another state could harm the United States. *See* Harold Edgar & Benno C. Schmidt, Jr., *The Espionage Statutes and Publication of Defense Information*, 73 COLUM. L. REV. 929, 987–88 (1973) (noting injury and advantage may be "surplusage" in the statute because of the connection between advantaging one state and harming the United States).

104. 18 U.S.C. § 794(a). This prohibition applies to ally and adversary nations. Jonathan Pollard was sentenced to life in prison for spying for Israel. He was released on parole in 2015 and in 2020 moved to Israel where he was welcomed as a hero by Prime Minister Benjamin Netanyahu. *See* David M. Halbfinger & Isabel Kershner, *Jonathan Pollard, Spy for Israel, Gets Hero's Welcome from Netanyahu: "You're Home,"* N.Y. TIMES (Dec. 30, 2020), https://www.nytimes.com/2020/12/30/world/middleeast/jonathan-pollard-israel-us-spy.html.

105. 18 U.S.C. § 794(b).

prohibits conspiracy to violate § 794(a)–(b).[106] All § 794 provisions permit a punishment of life imprisonment or death.[107]

In contrast, 18 U.S.C. § 793 provides broader prohibitions covering the "possession of, access to, [and] control over" such information and dissemination to anyone "not entitled to receive" it.[108] The Section prohibits the collection,[109] receipt,[110] or dissemination[111] of defense information; covering those who have authorized access,[112] unauthorized access,[113] and unauthorized receipt.[114] The Section also punishes those who conspire to violate the Act[115] and those with lawful access who lose information through gross negligence.[116] Violation of § 793 is punishable by ten years' imprisonment and a fine.[117]

Almost every aspect of §§ 793–794 has been litigated and upheld despite facial and as-applied constitutional challenges. The Act repeatedly survives constitutional challenges for vagueness,[118] with courts providing additional definitions to clarify the Act's broad language, such as the determination that information "relating to the national defense" need not be classified,[119] but must be "closely held by the government."[120] Such judicial clarifications of the Act's terms reinforce the Act's broad coverage and the judiciary's disinclination to restrict the Act's application.[121]

---

106. *Id.* § 794(c).
107. *Id.* § 794(a)–(c).
108. *Id.* § 793(d)–(e).
109. *Id.* § 793(a)–(b).
110. *Id.* § 793(c).
111. *Id.* § 793(d)–(e).
112. *Id.* § 793(d).
113. *Id.* § 793(e).
114. *Id.* § 793(c).
115. *Id.* § 793(g).
116. *Id.* § 793(f).
117. *Id.*
118. *See* Gorin v. United States, 312 U.S. 19, 27–28 (1941) (rejecting an argument that "national defense" was unconstitutionally vague, noting that it has a "well understood connotation" cognizable to a jury). *But see* Daniel Larsen, *Before "National Security": The Espionage Act of 1917 and the Concept of "National Defense,"* 12 HARV. NAT'L SEC. J. 329, 333–34 (2021) (adopting an originalist interpretation of the statute to conclude "national defense" has a distinct meaning from "national security," and, as understood at the Act's passage, "national defense" is narrower than "national security").
119. *See* United States v. Safford, 40 C.M.R. 528, 532 (A.B.R. 1969), *rev'd on other grounds*, 41 C.M.R. 33 (C.M.A. 1969); United States v. Allen, 31 M.J. 572, 627–28 (N-M C.M.R. 1990).
120. United States v. Morison, 844 F.2d 1057, 1076 (4th Cir. 1988), *cert. denied*, 486 U.S. 1306 (1988) (internal quotation marks omitted). Even publicly available information may still qualify under the Act unless it is made public by official government release. *See* United States v. Squillacote, 221 F.3d 542, 577–80 (4th Cir. 2000); *Allen*, 31 M.J. at 627–28; United States v. Marchetti, 466 F.2d 1309, 1318 (4th Cir. 1972) ("Rumor and speculation are not the equivalent of prior disclosure, however, and the presence of that kind of surmise should be no reason for avoidance of restraints upon confirmation from one in a position to know officially.").
121. For a comprehensive exploration of judicial opinions defining the Act's terms, see Fern L. Kletter, Annotation, *Validity, Construction, and Application of Federal Espionage Act, 18 U.S.C.A. §§ 793 to 794*, 59 A.L.R. Fed. 2d 303, §§ 18-27 (2011).

A central component to the Espionage Act is the mens rea requirement, which differs across provisions.[122] The necessary scienter under § 793(a)–(b) and § 794(a) is "intent or reason to believe that" the national defense-related information "*is to be used* to the injury of the United States, or to the advantage of any foreign nation."[123] The mens rea for § 793(a)–(b) and § 794(a) is a stricter requirement than other provisions of the Act by virtue of the "is to be used" language, which the Supreme Court determined to require "bad faith."[124] This higher scienter requirement conforms to the availability of a death sentence for violations of these provisions.

In contrast, § 793(d)–(e) requires a lesser standard of mens rea. These provisions punish one with lawful or unauthorized access who "willfully communicates, delivers, [or] transmits" information the possessor has "reason to believe *could be used*" to harm the United States or benefit another state.[125] The phrase "could be used" in these subsections establishes a lower mens rea requirement than "is to be used" from § 793(a)–(b) and § 794(a).[126] In contrast to knowing information "is to be used" to U.S. detriment, "could be used" merely requires the discloser be aware of the *potential* for the information to be used to U.S. detriment.[127] Sections 793(d)–(e) distinguish between tangible (e.g., "document[s]") and intangible (e.g., orally communicated) "information."[128] The "willfulness" mens rea standard applies to both, but the additional requirement of "reason to believe could be used to harm" applies only to the communication of intangible information.[129]

For tangible information, the mens rea is an even lower threshold, requiring only "willful" communication. This "willfulness" standard does not require a specific intent to harm the United States but instead requires a "conscious choice to communicate [the] covered information."[130] Thus, "willful" communication only requires the intent to disclose protected information, not the intent to harm.[131] As a result, courts have determined that a defendant's noble

122. Mens rea discussions vary across courts and provisions. For a succinct resource that captures the variations and details, see *id*. §§ 41–46.

123. 18 U.S.C. § 793(a)–(b); *id*. § 794(a) (emphasis added).

124. Gorin v. United States, 312 U.S. 19, 27–28 (1941).

125. 18 U.S.C. § 793(d)–(e) (emphasis added).

126. *See* United States v. Perkins, 47 C.M.R. 259, 263 (A.F.C.M.R. 1973) (noting Congress intended § 793(d) and (e) to have a lesser scienter requirement).

127. Mary-Rose Papandrea, *National Security Information Disclosures and the Role of Intent*, 56 WM. & MARY L. REV. 1381, 1398–99 (2015) [hereinafter Papandrea, *National Security Information*].

128. 18 U.S.C. § 793(d)–(e); *see* Kletter, *supra* note 121, §§ 42–43.

129. *See* United States v. Rosen, 445 F. Supp. 2d 602, 625–26 (E.D. Va. 2006).

130. United States v. Diaz, 69 M.J. 127, 132 (C.A.A.F. 2010).

131. *See* United States v. Miller, 874 F.2d 1255, 1277–78 (9th Cir. 1989) (finding the Supreme Court's statement in *Gorin* requiring "bad faith" allows conviction if the defendant "voluntarily and intentionally committed the acts charged"); United States v. Hung, 629 F.2d 908, 918–19 (4th Cir. 1980) (rejecting the argument that the Act requires "evil intent"); Papandrea, *National Security Information*, *supra* note 127, at 1400 (tracing the Supreme Court's interpretation of the term "willfully" across different criminal statutes to conclude Congress likely intended willful under the Espionage Act not to require intent to harm).

intentions[132] or patriotism[133] are irrelevant defenses. Furthermore, proof of actual harm from the disclosure is not required.[134] The *possibility* of harm is sufficient to violate § 793(d)–(e).

The Espionage Act does not cover only classified documents. While the classification of information is probative, it is not necessary to establish elements of espionage. As mentioned above, a document need not be classified to qualify as information "relating to the national defense,"[135] but its classification suggests a connection to national defense. Similarly, a document's classification is not necessary to establish the requisite mens rea for willful communication of information the "possessor has reason to believe could be used" to injure the United States or advantage another state.[136] However, classification is probative where classification status is determined by the risk of harm to national security.[137] Knowledge of the document's classification level then imputes knowledge of the risk of harm. Courts generally defer to executive assertions of the risk to national security.[138] Because of this deference, arguing information was misclassified is not a valid defense.[139]

Most leakers are charged under § 793(d), which applies to individuals with authorized possession of national security information.[140] As such, leakers need only intend to disclose documents to someone not entitled to receive them. Leakers providing oral information need only be aware of the potential damage from that information. Neither intent to harm nor proof of any harm is required.

C. Other Applicable Laws

The Espionage Act's broad applicability to all who disclose potentially harmful defense information is necessary for strong deterrence. Although the Espionage Act appears sweeping in the scope of its prohibitions, the Act is not the definitive authority criminalizing espionage activity. Acts of espionage may implicate the crime of treason, where disclosing sensitive information is giving "[e]nemies . . . [a]id

132. *See Diaz*, 69 M.J. at 134.

133. *See* United States v. Morison, 622 F. Supp. 1009, 1011 (D. Md. 1985), *aff'd*, 844 F.2d 1057 (4th Cir. 1988).

134. *See* United States v. Allen, 31 M.J. 572, 628 (N.M.C.M.R. 1990).

135. Gorin v. United States, 312 U.S. 19, 29 (1941); *see* United States v. Safford, 40 C.M.R. 528, 532 (A.B.R. 1969).

136. *See Diaz*, 69 M.J. at 132 (quoting 18 U.S.C. § 793(e)).

137. Classification levels are determined by the magnitude of harm resulting from unauthorized disclosure. Information is "confidential" for "damage" to national security, "secret" if "serious damage," and "top secret" if "exceptionally grave damage." *See* Exec. Order No. 13526, 75 Fed. Reg. 707 (Dec. 29, 2009).

138. *See Morison*, 844 F.2d at 1083 (Wilkinson, J., concurring) ("[T]he judicial role must be a deferential one because the alternative would be grave.").

139. *See* United States v. Lee, 589 F.2d 980, 990 (9th Cir. 1979) (finding that the defendant offering expert testimony to assist the jury in deciding whether the document was properly classified was "totally irrelevant").

140. *See* Mary-Rose Papandrea, *Leaker Traitor Whistleblower Spy: National Security Leaks and the First Amendment*, 94 B.U. L. REV. 449, 509 (2014) [hereinafter Papandrea, *Leaker Traitor*].

and [c]omfort."[141] Other laws apply to disclosure of specified information: diplomatic correspondence,[142] identity of covert intelligence officers and agents,[143] and nuclear energy and weapons information.[144] Different laws target the means of obtaining information: prohibiting theft or misuse of "thing[s] of value" owned by the government,[145] unauthorized computer access to classified information,[146] or unauthorized removal from secure facilities.[147] Other laws apply to specific individuals: government employees,[148] military personnel,[149] and foreign agents.[150]

This "patchwork"[151] of laws encompasses many of the activities subject to the Espionage Act. However, laws are better deterrents when punishment for violations are "swift, certain, and proportionate."[152] These laws are overlapping and carry varying punishments, impacting their deterrent value.[153] In contrast, the severe punishments available under the Espionage Act are proportionate to the immense harm espionage poses to national security and are necessary for adequate

141. *See* U.S. CONST. art. III, § 3 ("Treason against the United States, shall consist only in levying War against them, or in adhering to their Enemies, giving them Aid and Comfort."); 18 U.S.C. § 2381.

142. *See* 18 U.S.C. § 952.

143. *See* 50 U.S.C. § 3121(a)–(c).

144. *See* Atomic Energy Act of 1946, 42 U.S.C. § 2011.

145. 18 U.S.C. § 641.

146. *See id.* § 1030(a)(1).

147. *See id.* § 1924(a).

148. *See* 50 U.S.C. § 783(a) (prohibiting officers or employees of the United States from disclosing classified information to foreign agents); 18 U.S.C. § 219(a) (prohibiting public officials from acting as foreign agents without registering under the Foreign Agents Registration Act). Senator Robert Menendez was indicted under § 219 in October 2023 for conspiring to act as an agent of the Egyptian government. *See* Superseding Indictment at 41, United States v. Menendez, S1 23 Cr. 490 (S.D.N.Y. 2023). On July 16, 2024, he became the first U.S. Senator charged and convicted under § 219. *See* Adam Klasfeld, *Robert Menendez Guilty: The Significance of the First 'Foreign Agent' Conviction of a U.S. Senator*, JUST SEC. (July 19, 2024), https://www.justsecurity.org/97840/menendez-guilty-felony-convictions/.

149. The Uniform Code of Military Justice (UCMJ) prohibits espionage by reference to general crimes (UCMJ Art. 134) and establishes unique rules for communication with enemy forces (Art. 104 Aiding the Enemy). *See* 10 U.S.C. §§ 904, 934.

150. *See* 18 U.S.C. § 951(a) (criminalizing a foreign agent's failure to register with the government). On April 12, 2024, former U.S. Ambassador Victor Manuel Rocha pled guilty and was sentenced to prison for fifteen years for acting as an illegal agent of a foreign government under 18 U.S.C. § 951. *See* Press Release, Dep't of Just., Former U.S. Ambassador and National Security Council Official Admits to Secretly Acting as Agent of the Cuban Government and Receives 15-Year Sentence (Apr. 12, 2024), https://www.justice.gov/archives/opa/pr/former-us-ambassador-and-national-security-council-official-admits-secretly-acting-agent.

151. *See* MULLIGAN & ELSEA, *supra* note 95, at 30; *see also* Vladeck, *supra* note 80, at 219 ("As such, the statutory framework governing the complicated balance between governmental secrecy and the freedom of the press in the United States is little more than a disorganized amalgamation of unconnected statutes. Some of the provisions overlap each other and border on redundancy.").

152. *See* Kelli D. Tomlinson, *An Examination of Deterrence Theory: Where Do We Stand?*, 80 FED. PROB. 33, 33 (2016).

153. *Compare* 18 U.S.C. § 1924(a) (employee removing classified information is a misdemeanor offense punishable by maximum of five years), *with id.* § 951 (failing to register as a foreign agent carries maximum ten-year sentence).

deterrence.[154] Furthermore, the Act's broad application to many actions provides clearer prohibition than cross-referencing the numerous laws applicable to certain classes of individuals or types of information. Therefore, the Espionage Act likely supplies a greater deterrent effect than if the individual laws stood alone.

D. Special Considerations of Espionage Act Prosecutions

Not every unauthorized disclosure is prosecuted.[155] Numerous factors impact the decision to prosecute espionage. Notably, the need to further disclose protected information to effectively adjudicate cases majorly restricts espionage prosecutions. Protected information may be required for the prosecution to prove the elements of the crime or for the defendant to properly defend against accusations.

First, a defendant's constitutionally protected right to due process may require the use of classified information to present a defense. However, a defendant may abuse this right. For instance, a defendant may "graymail" the government by threatening to disclose additional classified information as part of their defense.[156] This threat of releasing unnecessary classified information is used as leverage to force the prosecutor to offer a plea bargain or to drop the case.[157] The Classified Information Protection Act (CIPA) mitigates the threat of graymail and enacts procedures to determine whether the use of classified information is necessary to satisfy the defendant's due process rights. In general terms, CIPA requires a pre-trial, closed hearing to determine whether a defendant's use of classified information may be disclosed without harming national security.[158] The judge determines whether the defendant's information is necessary to the defense and whether the prosecution may produce a viable, unclassified substitute.[159] CIPA determinations greatly define the contours of both sides' cases-in-chief.

Second, whether the disclosures are necessary for due process or are used as a bargaining chip, concerns for further disclosure of classified information dictate prosecutions. Some cases may not be pursued because effective prosecution could require additional disclosures.[160] Every prosecution under the Act requires this determination, and the government must decide whether proceeding with a prosecution is

---

154. *See* Edgar & Schmidt, *supra* note 103, at 1084; Leslie S. Edmondson, *Espionage in Transnational Law*, 5 VAND. L. REV. 434, 443 (1972) ("Prosecution under a less severe municipal law may not be satisfactory, since conviction on a minor charge will not serve as an effective deterrent to breaches of national security.").

155. *See* Papandrea, *Leaker Traitor*, *supra* note 140, at 462.

156. *See* David Ryan, *National Security Leaks, The Espionage Act, and Prosecutorial Discretion*, 6 HOMELAND & NAT'L SEC. L. REV. 59, 78–79 (2018).

157. *See* Karen H. Greve, *Graymail: The Disclose or Dismiss Dilemma in Criminal Prosecutions*, 31 CASE W. RSRV. L. REV. 84, 85–86, 92 (1980).

158. *See* Ryan, *supra* note 156, at 78–79.

159. *See id*.

160. *See* Papandrea, *Leaker Traitor*, *supra* note 140, at 457 ("In the past, government officials pursued few leak prosecutions out of the fear that more harm than good would come from the prosecution; they might have to reveal even more sensitive information in order to demonstrate that the information was properly classified and damaging to U.S. national security interests."); James Bruce, *The Consequences of Permissive Neglect: Laws and Leaks of Classified Intelligence*, 47 STUD. INTEL. 1, 15 (2003) ("The US government has shown a debilitating

worth further disclosure of classified information, which may compound the harm the government intends to rectify.

Additionally, critics of the Espionage Act claim that no harm actually befalls the United States following the disclosure of classified material.[161] Without proof of harm, prosecutions may appear unnecessary or even arbitrary, allowing critics to claim that the purpose of prosecutions is not to vindicate the harm to the United States but to wrongfully retaliate against the defendant.[162] However, proof of the true extent of harm is likely classified.[163] As a result, the government lacks the ability to defend its decision to prosecute because prosecutors are unable to publicly argue for the true extent of the damage done to national security from the disclosures.[164] Thus, what appears as blind deference to the executive branch's assertions of harm is really the necessary result of ensuring espionage may be punished without furthering the exact harm to national security that the law seeks to prevent.

The inherent intricacies of meeting the burden of proof in espionage cases requires prosecutors to be selective in the cases pursued. Prosecutions may then appear malicious, not because of personal animosity toward the defendant, but because of broader national security concerns. Yet, without the ability to defend these decisions to the public, belief that prosecutions are arbitrary continues unabated. This general distrust of the legitimacy of prosecutions then prompts calls to reform the Espionage Act.

III. RECONCILING PERCEPTION WITH REALITY: A HOLISTIC APPROACH TO ESPIONAGE

On August 13, 2022, Senator Rand Paul called for the repeal of the Espionage Act as an "egregious affront to the [First] Amendment."[165] While Senator Paul appears to be the sole government official advocating for complete repeal, there are numerous proposals to reform the Espionage Act, especially as it is applied to

---

reluctance to pursue legal remedies for the most serious leaks partly because subsequent courtroom publicity of sensitive information subverts its first objective of protecting such information from further disclosures.").

161. *See* Papandrea, *Leaker Traitor*, *supra* note 140, at 458; William H. Freivogel, *Publishing National Security Secrets: The Case for "Benign Indeterminacy,"* 3 J. NAT'L SEC. L. & POL'Y 95, 98–99 (2009) ("As for the claims of administration officials, there is scant evidence that national security has been harmed in any significant way by the disclosure of government secrets."); Bruce, *supra* note 160, at 3 ("It is a myth, too commonly held outside the Intelligence Community (IC), that leaks really do not do much harm.").

162. *See* Pamela Takefman, Note, *Curbing Overzealous Prosecution of the Espionage Act: Thomas Andrews Drake and the Case for Judicial Intervention at Sentencing*, 25 CARDOZO L. REV. 897, 911 (2013) (arguing the charges were "a pretext to retaliate against Drake for leaking").

163. *See* Bruce, *supra* note 160, at 2.

164. *See id.* ("It thus seems daunting to make a persuasive public case for legal correctives to address unauthorized disclosures when so little of the evidence for it can be discussed publicly. Proponents for better laws . . . sometimes feel that this is not a fair fight.").

165. *See* Juliana Kim, *Sen. Rand Paul Wants To Repeal the Espionage Act Amid the Mar-a-Lago Investigation*, NAT'L PUB. RADIO (Aug. 15, 2022, 5:00 AM), https://www.npr.org/2022/08/15/1117457622/rand-paul-what-is-espionage-act-repeal.

leakers.[166] Debate surrounding the Espionage Act is often bifurcated by interest. Its supporters tout national security and intelligence operations, while its critics herald free speech and press. The former often fail to acknowledge the importance of relevant constitutional protections, while the latter often dismiss the need for counterintelligence to keep the country secure. To bridge this gap, this Part contextualizes proposed reforms within the practice of espionage. Adopting a holistic approach to espionage, this Part argues against the wisdom of proposed reforms to the Act. This Part first discusses how both spying and leaking implicate the essential components of espionage: the ease of disseminating information with current technology, the need to protect and recruit intelligence sources, and the harm that results from covertly and publicly disclosed secrets. This Part then argues against the efficacy of proposed reforms to the Act that seek to differentiate between spies and leakers. Because spies and leakers engage in similar activities that materially impact national security, proposals to exclude leakers from the Espionage Act because of First Amendment protections, a supposed intent to benefit the public, or a benefit-harm balancing test are unworkable in practice and undercut the Act's purpose.

A. Updating Public Understanding of Modern Espionage

As the maxim goes, espionage is the second oldest profession.[167] Yet the practice of espionage has drastically changed over the years.[168] Technological advances have eased the ability to access and transmit critical information. Even with these advances, however, the crucial need to protect intelligence sources and prevent severe harm resulting from divulged secrets remains.

1. Technology Facilitates Disclosures

The term "espionage" likely conjures images of covert messages left with chalk marks, documents wrapped in plastic bags left at dead drops, and substantial amounts of cash delivered as payment.[169] However, technology has transformed this type of "cloak-and-dagger" spying[170] into bits-and-bytes spying. The same plastic-wrapped documents may now be downloaded *en masse* and sent electronically to any number of recipients.[171] Rather than uncovering the foreign handler recruiting spies or

166. *See, e.g.*, Takefman, *supra* note 162, at 900; Kitrosser & Schulz, *supra* note 18, at 156; Lindsay Barnes, *The Changing Face of Espionage: Modern Times Call for Amending the Espionage Act*, 46 MCGEORGE L. REV. 511, 516 (2014).

167. *See* Chesterman, *supra* note 45, at 1072.

168. *See* Terry, *supra* note 34, at 392; Edmondson, *supra* note 154, at 434.

169. These were all activities undertaken by Robert Hanssen while spying for the Soviets. Hanssen, and other spies, commonly exchanged information via dead drops, which are prearranged locations where a spy leaves documents for his handler to later retrieve. *See* Baker, *supra* note 1.

170. *See* Terry, *supra* note 34, at 392; *see also* Krizek, *supra* note 75, at 350–51.

171. *See* David Gioe, *Tinker, Tailor, Leaker, Spy*, NAT'L INT., Jan.–Feb. 2014, at 51, 58–59 (noting a "new dimension in espionage" with Snowden and Mannings' mass disclosures of classified information).

surveilling an employee with an unexplained infusion of cash, counterintelligence work now often resides at the access point to protected information.[172]

Laws criminalizing espionage have similarly evolved to prohibit accessing and revealing information, not just the use of deception or operating as a state agent.[173] Although not obsolete, a foreign handler running an agent and operating as the conduit to transmit information is no longer strictly necessary. Now, all one needs is a USB-drive and an adversary's email address to spy. A leaker engages in the same unauthorized access and instead sends documents to a journalist's email or uploads to WikiLeaks.[174] Thus, the actions of spying and leaking are functionally equivalent, save for the recipient's email address. The ease of downloading and transmitting information electronically drastically decreases the barrier to disseminate protected information and engage in espionage.

2. The Need To Protect Current and Future "Sources and Methods"

The ease of communicating vital intelligence does not diminish the value of that intelligence. U.S. foreign policy relies on intelligence collected from a myriad of sources, which must be protected to ensure continued intelligence production. National security practitioners routinely cite "sources and methods" to justify classifying specific information.[175] The term's overuse inoculates the public to the true meaning of the term.[176] Simply put, sources and methods refer to the individuals and tools used to cultivate vital information.[177]

Protecting these sources and methods is essential to U.S. intelligence operations, and compromising sources and methods can have grave, long-term impacts. Hanssen's disclosures resulted in identification of U.S. spies operating in the U.S.S.R.[178] Three were imprisoned; two were executed.[179] Similarly, Teixeira's recent disclosures demonstrate the extent U.S. spies infiltrate policy circles and reveal

172. *See* Krizek, *supra* note 75, at 350–51 ("In modern times, espionage has been institutionalized, becoming primarily the unauthorized disclosure and transfer of information that a State has reason to keep secret.").

173. Laws prohibiting these activities still exist, but they are not the focus of the Espionage Act. *See* Edmondson, *supra* note 154, at 451–52.

174. *See* Mark Fenster, *The Elusive Ethics of Leaking*, 18 GEO. J. INT'L AFFS. 112, 112 (2017) (noting leakers "can now avoid the bottlenecks to disclosure that the established, institutional media once imposed by distributing their leaks via new news outlets and leak intermediaries like WikiLeaks").

175. *See* Bruce, *supra* note 160, at 1 ("The future of [U.S.] Intelligence effectiveness depends to a very significant degree on keeping its secrets about collection sources and methods and analytical techniques.").

176. *See* Gary Keeley, *The Imperative of Intelligence Services To Protect from Exposure the Sources and Methods of Intelligence Collection*, J. U.S. INTEL. ST., Winter–Spring 2022, at 7, 9 ("If the awareness of the centrality of the protection of intelligence sources and methods is too often vague or unwelcome to those outside of the profession of intelligence, it is clear to intelligence professionals.").

177. *See id.* at 7.

178. *See* Kayla Epstein, *Robert Hanssen: The Fake Job that Snared FBI Agent Who Spied for Moscow*, BBC (June 6, 2023), https://www.bbc.com/news/world-us-canada-65820220.

179. *Id.*

capabilities of advanced satellite systems.[180] These disclosures exposed sources and methods developed with significant time and cost that may now be unable to produce further intelligence.[181] Additionally, disclosing methods of intelligence gathering informs adversaries how best to evade surveillance. Following a 1998 leak revealing the NSA's ability to eavesdrop on Osama bin Laden's satellite phone, bin Laden "stopped using it."[182] A direct line to bin Laden in the years preceding September 11, 2001, would have been invaluable. Yet this potential advantage was dashed due to a leak revealing sources and methods.

Leaks not only offer free intelligence to adversaries,[183] they impede U.S. efforts to cultivate future sources.[184] Because of the universal criminalization of espionage in domestic law and the severity of punishment if caught, deciding to spy for the United States is a serious decision.[185] Sources put their lives on the line and must be confident that the United States can adequately protect them.[186] In *Snepp v. United States*, the Supreme Court recognized the imperative of protecting these sources: "The continued availability of these foreign sources depends upon the CIA's ability to guarantee the security of information that might compromise them and even endanger the personal safety of foreign agents."[187] Leaks of classified information threaten to expose information that may identify that source, undermining the credibility of an intelligence officer's promise of protection.[188]

The intelligence community understands the imperative to safeguard sources' identities, but these efforts may be inadequate. Restricting access to sources'

---

180. *See* Edward Helmore & Julian Borger, *Jack Teixeira, Suspect in Pentagon Leaks, Charged Under Espionage* Act, GUARDIAN (Apr. 14, 2023, 1:39 PM), https://www.theguardian.com/us-news/2023/apr/14/jack-teixeira-charged-pentagon-leaks-espionage-act; *see also* Shane Harris & Dan Lamothe, *Intelligence Leak Exposes U.S. Spying on Adversaries and Allies*, WASH. POST (Apr. 8, 2023, 7:48 PM), https://www.washingtonpost.com/national-security/2023/04/08/intelligence-leak-documents-ukraine-pentagon/ ("[U.S. officials] indicated that LAPIS [satellite system] was among the more closely guarded capabilities in the U.S. intelligence arsenal.").

181. *See* Helmore & Borger, *supra* note 180; Harris & Lamothe, *supra* note 180.

182. *See* Bruce, *supra* note 160, at 7 (quoting former White House press spokesman Ari Fleischer, Bruce continues, "[w]hat the public cannot easily know, because the overwhelming bulk of this intelligence must necessarily remain classified, is that the bin Laden example cited here is just the tip of the iceberg").

183. *See id.*

184. *See* Gioe, *supra* note 171, at 51 ("[Manning's and Snowden's disclosures] seriously impeded America's future ability to recruit foreign sources . . . .").

185. *See id.* at 53 ("Indeed, any slipup on the part of the recruiting officer, such as indiscretion or sloppy agent tradecraft, could very well cost the foreign agent his life and potentially even jeopardize the well-being of his family in his home country.").

186. *See id.* ("The potential agent must be satisfied that the Americans can assure his safety, and, of course, these assurances must be credible.").

187. *See* 444 U.S. 507, 512 (1980) (per curiam) (finding a former CIA employee breached his contract with the CIA by publishing a book without obtaining prior CIA approval and was thus not entitled to the book's profits).

188. *See* Papandrea, *National Security Information*, *supra* note 127, at 1410 ("The government has argued that any breaches of confidentiality harm the United States because the breaches send a message to our friends and allies alike that we cannot be trusted.").

identities to only those with a "need to know" helps protects sources.[189] However, potential recruits are likely unaware of internal classification procedures and may believe that their identity is widely available, increasing the risk of compromise if any one of them decides to leak.[190] Thus, the Supreme Court recognized that the very "appearance of confidentiality" is essential to ensure continued sources of vital intelligence.[191] Any leak, no matter how tangential to an agent, diminishes all agents' trust in the promise of safety and may result in many declining to accept the risk.

3. The Harm Exists in Covert and Public Disclosures

In addition to compromising sources and methods, disclosures can cause tangible harm to the United States. As discussed above, the extent and contours of damage to U.S. security will likely remain classified, yet this harm exists whether a spy or a leaker releases the information.[192] Simply put, the information is compromised whether an adversary reads it in a document delivered via dead drop or in a U.S. newspaper. Hopes that public disclosures do not harm national security rely on the argument that adversarial intelligence services are not aware of every piece of information disclosed by the media. In short: "[d]ifferences in the detrimental consequences of the breach lie primarily in the hope that foreigners do not read carefully."[193] Although this hope was—luckily—realized during WWII, this hope is now futile. During WWII, Japanese officials overlooked a story in the *Chicago Tribune* stating the U.S. had uncovered Japanese codes.[194] If read, Japanese forces would have updated their codes, destroying a key strategic advantage during the war. Today, adversaries have easy access to media and often are "close and voracious readers" of U.S. media.[195]

The concept of "open source intelligence" confirms this conclusion. The Central Intelligence Agency employs Open Source Collection Specialists,[196] recognizing that "[c]ollecting intelligence these days is at times less a matter of stealing

189. *See* Keeley, *supra* note 176, at 7.

190. *See* Gioe, *supra* note 171, at 53 ("[I]n all cases potential sources must be reassured that hushed words stated in confidence won't endanger them in the next tranche of leaked information.").

191. *See Snepp*, 444 U.S. at 509 n.3.

192. *See* United States v. Morison, 604 F. Supp. 655, 660 (D. Md. 1985). The *Morison* court explained:

> [T]he danger to the United States is just as great when this information is released to the press as when it is released to an agent of a foreign government. . . . [The] fear is realized whether the information is released to the world at large or whether it is released only to specific spies.

Id.

193. *See* Edgar & Schmidt, *supra* note 103, at 934.

194. *See* Papandrea, *National Security Information*, *supra* note 127, at 1435.

195. Bruce, *supra* note 160, at 4; *see also* Papandrea, *National Security Information*, *supra* note 127, at 1434 ("Foreigners read our papers, watch our television programs, and search U.S. websites to obtain information they would never be able to collect on their own.").

196. *See Open Source Collection Specialist,* CENT. INTEL. AGENCY, https://www.cia.gov/careers/jobs/open-source-collection-specialist/ (last visited Jan. 8, 2025).

through dark alleys in a foreign land to meet some secret agent than one of surfing the Internet under the fluorescent lights of an office cubicle to find some open source."[197] The sheer number of websites and social media platforms guarantees easy access to global information.[198] The U.S. understands the importance of open source intelligence, but so do its adversaries.[199] As one example, members of the Wagner Group, a Russian paramilitary organization, were caught attempting to gain access to video game servers as it is increasingly common for gamers to release classified information to settle arguments with other players about in-game weapons specifications.[200] Possessing accurate specifications may advantage an adversary in current or future conflicts employing those weapons. Thus, the public disclosure of classified information, even if to a seemingly innocent group of people in an online chat, has tangible national security implications.

Any arguments to meaningfully differentiate the harm between public and covert disclosure fail upon closer scrutiny. Some argue that the harm is greater when a spy divulges information because a spy's disclosure is covert.[201] They assert the United States continues to operate on the belief that the disclosed information is secret, oblivious to the damage caused.[202] In contrast, leakers expose secrets publicly, and the government knows what information was compromised and can take measures to mitigate any harm.[203]

While the harm between public and covert disclosure undoubtedly differs, the harm exists regardless. Consider a hypothetical surveillance capability the United States employs against adversaries abroad. A spy disclosing its existence to an adversary allows that adversary to adopt countermeasures to avoid surveillance. The adversary may additionally exploit that capability to pump out misinformation—causing the intelligence community to waste valuable resources chasing down falsities. Once the disclosure is discovered, the United States must then review every potentially compromised piece of information and expend even more resources to replace the lost capability. In contrast, public disclosure of the capability may spare

197. *See* Stephen Mercado, *Sailing the Sea of OSINT in the Information Age*, 48 STUD. INTEL. 45, 45 (2004).

198. *See id*. at 47–48.

199. *See* Bruce, *supra* note 160, at 4 ("Classified intelligence disclosed in the press is the effective equivalent of intelligence gathered through foreign espionage.").

200. *See* Jonathan Askonas & Renée DiResta, *How Gamers Eclipsed Spies as an Intelligence Threat*, FOREIGN POL'Y (Apr. 15, 2023, 7:00 AM), https://foreignpolicy.com/2023/04/15/ukraine-leak-intelligence-discord-espionage-gamers-internet-online/. The FBI has also issued warnings on the dangers of social media and the ability for adversaries to manipulate users to obtain information. *See* FBI, *Internet Social Networking Risks*, DEP'T OF JUST., https://www.fbi.gov/file-repository/internet-social-networking-risks-1.pdf/view (last visited Jan. 8, 2025).

201. *See* Papandrea, *Leaker Traitor*, *supra* note 140, at 488; *see also* Geoffrey R. Stone, *Government Secrecy vs. Freedom of the Press,* 1 HARV. L. & POL'Y REV. 185, 216 (2007).

202. *See* Harold Edgar & Benno C. Schmidt Jr., Curtiss-Wright *Comes Home: Executive Power and National Security Secrecy*, 21 HARV. C.R.-C.L. L. REV. 349, 401 (1986) ("The greatest damage occurs when the government believes that 'secrets are secret.'").

203. *See* Papandrea, *Leaker Traitor*, *supra* note 140, at 540 ("[T]he government knows what the enemies know.").

the harm arising from adversaries exploiting the compromised capability. However, the harms incurred in a public disclosure from lost intelligence and expending resources to establish similar capabilities remain. Furthermore, when the identity of a source is covertly revealed, the individual is in immediate danger, though they may not realize they are compromised until they are apprehended.[204] If their identity is publicly revealed, they may have a chance to retreat to safety. However, the public disclosure endangers others because every interaction with that individual is now tinged by the connection to intelligence operations.[205] The disclosure also compromises the viability and strength of other sources' covers by publicly revealing details of intelligence agencies' extensive efforts to craft and maintain covers.[206] Covert and public disclosures cause tangible harm to the sources and methods of intelligence.

Whether the magnitude of the harms differ between covert or public disclosure is immaterial to the conclusion that both disclosures are harmful and thus worthy of deterrence. Furthermore, the Espionage Act implicitly recognizes this harm differential where disclosure to foreign agents is punishable by life in prison or death, whereas disclosure to undisclosed recipients, including the media, is punishable by ten-years' imprisonment.[207] No leakers have been prosecuted under § 794, which carries the more severe penalties.[208] Therefore, the difference in harm between public and covert disclosure operates in the degree of punishment, not in absolving an offender from liability entirely.

Understanding the current practice of intelligence gathering leads to the conclusion that spies and leakers engage in the same activity: espionage. Both spies and leakers disclose protected information that harms national security. Whether this information is obtained by one state or every state with access to the internet, the activity and the harm remain the same: the source's life is at risk and the methods of collection are exposed. The very fact that Russia offered Snowden citizenship suggests the extent to which Russia values his disclosures.[209] Thus, any justifiable distinction between these actions could only be found in the motive for or the recipient of the disclosure.

---

204. CIA's Aldrich Ames divulged the identities of sources operating within the Soviet Union. Ten were executed. Others were imprisoned. *See* David Wise, *Victims of Aldrich Ames*, TIME (May 22, 1995, 12:00 AM), https://time.com/archive/6727449/victims-of-aldrich-ames/.

205. For example, a 2003 news article revealed Valerie Plame's identity as a CIA covert operations officer. Following the disclosure of her identity, she discussed the end of her own career as well as the impact on those she encountered, noting national security breaches "ha[ve] jeopardized and even destroyed entire networks of foreign agents, who in turn risk their own lives and those of their families to provide the United States with needed intelligence. Lives are literally at stake." *See Transcript: CIA Leak Investigation*, *House Oversight and Government Reform Committee*, C-SPAN (Mar. 16, 2007), https://www.c-span.org/video/?197169-1/cia-leak-investigation.

206. *See* Stephen Smith, *The Exposure of Valerie Plame*, CBS NEWS (Oct. 28, 2005, 9:09 PM), https://www.cbsnews.com/news/the-exposure-of-valerie-plame/.

207. *See* 18 U.S.C. §§ 793, 794; Papandrea, *National Security Information*, *supra* note 127, at 1417.

208. *See* Papandrea, *Leaker Traitor*, *supra* note 140, at 509; 18 U.S.C. §§ 793, 794.

209. *See* Smith, *supra* note 2.

B. Responding to Attempts To Distinguish Spies and Leakers

Where the actions of spies and leakers both involve the disclosure of information, opponents of the Espionage Act target their criticism to provisions other than unauthorized disclosure. Calls for reform typically emphasize First Amendment protections of free speech and press, intent requirements, or weighing the harm versus benefit of the disclosure. This Section outlines the contours of these arguments to conclude that there is no principled avenue to distinguish leakers without inhibiting the Act's deterrent factor for spies.

1. The First Amendment

One common argument against the Espionage Act's application to leakers is the assertion that the First Amendment protects leakers' actions. Considering that spies and leakers engage in similar activities, extending First Amendment protection to leakers without extending protection to spies is illogical. Advocates for amending the Act acknowledge that there is no right to disclose secrets to a foreign agent, but they nonetheless vigorously contend that the Act violates a leaker's right to speak freely. Distinguishing these two types of speech is often superficial—referencing an obvious, inherent difference in the two types of speech.[210] However, closer examination of the First Amendment precludes concluding that speech divulging secrets is protected as long as it is done publicly.

First Amendment jurisprudence correctly balances the inherent tension between mandating secrecy for national security and protecting the right to free speech and press. There are no Supreme Court cases deciding the First Amendment implications of the Espionage Act.[211] Yet lower court decisions confirm the Act's constitutionality. To start, espionage may sidestep First Amendment protections entirely where spies' and leakers' actions are more correctly characterized as "theft" of information, not speech.[212] Thus, spies' and leakers' actions avoid any First Amendment protection.

Even if some acts of espionage are considered speech, applicable Supreme Court cases support the constitutionality of the Act's prohibitions. The Supreme Court restricts government employees' free speech protections when the speech

---

210. *See* Papandrea, *Leaker Traitor*, *supra* note 140, at 453 ("The First Amendment should support the common sense distinction between those who leak information with the purpose and effect of contributing to the public debate, and those who engage in espionage or even treason by giving national security information to foreign countries or organizations."). Other arguments attempt to distinguish the types because disclosures in secret do not contribute to public debate. *See id.* at 516 ("Traditional espionage involves the secret exchange of information; accordingly, by definition, it does not contribute to the marketplace of ideas and cannot be said to promote self-government and deliberation." (footnote omitted)).

211. The Supreme Court denied certiorari in Morison's case, which provides the foundational jurisprudence for the prosecution of leakers. *See* Morison v. United States, 488 U.S. 908, 908 (1988).

212. *See* United States v. Morison, 844 F.2d 1057, 1069–70 (4th Cir. 1988), *cert. denied,* 488 U.S. 908 (1988) (noting the defendant is "not entitled to invoke the First Amendment as a shield to immunize his act of thievery").

"owes its existence to a public employee's professional responsibilities."[213] Sensitive national security information is available only to individuals granted access by virtue of their employment.[214] Thus, speech concerning classified content is rightly credited to the employee's professional responsibilities and may be appropriately exempt from First Amendment protections altogether.[215] For classified information specifically, the Supreme Court upheld the constitutionality of pre-publication review for employees seeking to discuss their government work.[216] These restrictions clearly infringe on government employees' ability to participate in public debate to the full extent that their personal knowledge would allow. However, public employment and access to classified information is a privilege, not a right.[217] A cost of this privilege is greater restriction on the ability to disclose information learned only by virtue of employment. Thus, whether it is prohibiting a government employee from selling information to a foreign agent or sending documents to a newspaper, these restrictions are attendant to the privilege of learning the information in the first place. If someone does not want to accept these common-sense restrictions on revealing sensitive information, they should not be allowed access to the information in the first place. Thus, the Espionage Act does not infringe on general free speech rights but instead gives weight to the privilege and responsibility of being entrusted with the nation's secrets.

Furthermore, general First Amendment doctrine supports restrictions on disclosures. Content-based speech restrictions may only be upheld upon showing that the restrictions are narrowly tailored to achieve a compelling government interest.[218] The Supreme Court has asserted that there is "no governmental interest more compelling than the security of the Nation."[219] Restrictions on speech tailored to

---

213. *See* Garcetti v. Ceballos, 547 U.S. 410, 411 (2006); *see also* Bd. of Cnty. Comm'rs v. Umbehr, 518 U.S. 668, 668 (1996) (holding independent contractors are subject to the same First Amendment framework as government employees).

214. *See Security Clearance Process*, U.S. INTEL. CMTY. CAREERS, https://www.intelligencecareers.gov/usa/security-clearance-process (last visited Jan. 9, 2025).

215. *See* Stephen I. Vladeck, *The Espionage Act and National Security Whistleblowing After* Garcetti, 57 AM. U. L. REV. 1531, 1535 (2008) (noting the disclosure of classified information "would undoubtedly constitute speech that could not have existed but for the 'public employee's professional responsibilities'").

216. *See* Snepp v. United States, 444 U.S. 507, 509 n.3 (1980) (per curiam) (holding pre-publication review is not an unconstitutional prior restraint on protected speech); United States v. Marchetti, 466 F.2d 1309, 1318 (4th Cir. 1972) (same).

217. *See* Press Release, Dep't of Just., Former U.S. Ambassador and National Security Council Official Charged with Secretly Acting as an Agent of the Cuban Government (Dec. 4, 2023), https://www.justice.gov/opa/pr/former-us-ambassador-and-national-security-council-official-charged-secretly-acting-agent ("Those who have the privilege of serving in the government of the United States are given an enormous amount of trust by the public we serve."). The privilege, not right, to public service was also confirmed by Oliver Wendell Holmes while he was on the Massachusetts Supreme Judicial Court. *See* McAuliffe v. Mayor of New Bedford, 29 N.E. 517, 517 (Mass. 1892) ("The petitioner may have a constitutional right to talk politics, but he has no constitutional right to be a policeman.").

218. *See* David Hudson, *Strict Scrutiny*, FREE SPEECH CTR. (July 2, 2024), https://firstamendment.mtsu.edu/article/strict-scrutiny/.

219. Haig v. Agee, 453 U.S. 280, 307 (1981).

promote national security concerns have survived this strict scrutiny,[220] making it likely that the Supreme Court would similarly hold that deterring espionage and guarding against its harms are sufficiently compelling to restrict disclosure of protected information. As discussed above, the harm resulting from seemingly innocuous disclosures emphasizes the importance of these restrictions to national security. Considering the unique privilege of accessing sensitive information and the magnitude of harm resulting from its disclosure, restrictions on this information's disclosure is necessary and aligns with current First Amendment jurisprudence.

In addition to speech, critics contend that the Espionage Act is an unconstitutional infringement on free press. The precise contours of the Espionage Act as applied to members of the press for publishing protected information remain opaque because there have never been any prosecutions to warrant clarifying judicial decisions.[221] However, Justice White's concurring opinion in *New York Times v. United States* suggests that the press could be prosecuted for publishing classified information.[222]

Laws prohibiting the press from committing crimes are not per se violations of the First Amendment. It is argued that where free press requires access to information of public concern, criminalizing leaks inhibits newsgathering activities.[223] However, effective newsgathering does not give license to journalists to violate laws[224] nor does it guarantee access to private information.[225] The First Amendment does, however, protect the publication of information received from a third party who obtained the material illegally.[226] Whether this protection extends to information received in violation of the Espionage Act's prohibition on the receipt of protected information[227] remains untested because there have been no prosecutions of the media for passively receiving information.

---

220. *See* Holder v. Humanitarian Law Project, 561 U.S. 1, 36 (2010).

221. *Morison* is the only appellate decision on leaking to the press. *See* Kitrosser & Schulz, *supra* note 18, at 185.

222. *See* 403 U.S. 713, 740 (1971) (White, J., concurring). Justice White continues, noting:

> I am not, of course, saying that either of these newspapers has yet committed a crime or that either would commit a crime if it published all the material now in its possession. That matter must await resolution in the context of a criminal proceeding if one is instituted by the United States.

Id.

223. *See* Kitrosser & Schulz, *supra* note 18, at 181–82.

224. *See* Branzburg v. Hayes, 408 U.S. 665, 691 (1972) ("It would be frivolous to assert . . . that the First Amendment, in the interest of securing news or otherwise, confers a license on either the reporter or his news sources to violate valid criminal laws."); Stone, *supra* note 201, at 209. Stone writes:

> In some circumstances, journalists would be better able to discover valuable information if they could wiretap the offices of senators or burgle the homes of corporate executives. But I doubt we are about to hold wiretapping, trespass, and burglary laws unconstitutional as applied to journalists (though such a claim is not absurd).

Id.

225. *See Branzburg*, 408 U.S. at 684.

226. *See* Bartnicki v. Vopper, 532 U.S. 514, 527–28 (2001).

227. *See* 18 U.S.C. § 793.

There have only been two prosecutions under the Espionage Act for individuals not responsible for the original disclosure. In 2005, two employees of American Israel Public Affairs Committee (AIPAC) were indicted for receipt of information disclosed to them by a Department of Defense official.[228] The case was later dropped.[229] In 2018, WikiLeaks founder Julian Assange was indicted for activities associated with Chelsea Manning's disclosures.[230] Critics of the indictment argue that it targets legitimate newsgathering activities essential for a free press.[231] However, Assange's superseding indictment, filed in June of 2020, asserts activity beyond passive receipt of classified materials and alleges an active role in soliciting disclosures in violation of the Espionage Act.[232] In June 2024, Assange pleaded guilty to one count of violating the Espionage Act.[233]

Prosecuting the receipt of information raises concerns that journalists will refrain from legitimate newsgathering activities for fear of criminal liability.[234] Yet, concerns over this chilling effect react to a problem that has not yet materialized. The importance of clearly protecting legitimate newsgathering is discussed below. Even so, staunch critics of the Act admit there is no absolute right to publish any information.[235] There are some categories of information that pose so great a danger that the First Amendment does not protect the disclosure.[236] This category may just expand if critics and the public at large understand the full extent of harms resulting from seemingly innocent disclosures.

However disconcerting it may be that an individual can restrict someone's right to discuss and publish information by placing a "Classified" stamp on a document, this restriction is necessary for national security. Any other determination would render the classification system moot. The government would be unable to protect any information, even the most sensitive national secrets, if anyone could disclose protected information in order to discuss matters of public interest. Even traditional First Amendment principles, such as the maxim: "the antidote to bad speech is

228. *See* Kitrosser & Schulz, *supra* note 18, at 177.

229. *See id.* at 178.

230. *See* Indictment at 1, United States v. Assange, 2018 WL 7982975 (E.D. Va. Mar. 6, 2018) (No. 1:18CR00111).

231. *See* MULLIGAN & ELSEA, *supra* note 95, at 27–28.

232. *See* Superseding Indictment at 1–2, United States v. Assange, 2020 WL 3468372 (E.D. Va. June 24, 2020) (No. 1:18CR00111).

233. *See* Charlie Savage, *Assange's Plea Deal Sets a Chilling Precedent, but It Could Have Been Worse*, N.Y. TIMES (June 25, 2024), https://www.nytimes.com/2024/06/25/us/politics/assange-plea-deal-press-freedom.html.

234. *See* Vladeck, *supra* note 80, at 235.

235. *See, e.g.*, *id.* at 237 ("There is some information, such as details on how to construct nuclear weapons, to which I recognize absolutely no public right . . . .").

236. Near v. Minnesota, 283 U.S. 697, 716 (1931) (concluding the government may prevent publication of the "sailing dates of transports" or the "location of troops"); United States v. Progressive, Inc., 467 F. Supp. 990, 998, 1000 (W.D. Wis. 1979) (enjoining publication of an article "The H-Bomb Secret How We Got It, Why We're Telling It").

more speech,"[237] are often inapplicable to classified information where a burned source or a now-defunct collection method cannot be rectified with more speech. Once the bell is rung, it cannot be unrung. When it comes to national security, that bell can cause disastrous harm.

2. Intent

Another common proposal for absolving leakers of Espionage Act liability is to alter the requisite mens rea under the Espionage Act to require specific intent to harm the United States, theoretically releasing leakers from liability. However, any alteration in the required mens rea would be untenable in practice and would likely decrease the Act's deterrent power.

The common perception is that spies are motivated to harm the United States, while leakers are motivated to inform public debate. However, analysis of the motives of both spies and leakers precludes such a clear delineation.[238] Classic spies may avoid clear determination of their motives. Longstanding approaches to recruit foreign sources appeal to money, ideology, coercion, or ego.[239] As these categories suggest, spies may often be recruited for entirely self-interested reasons: the promise of monetary reward or to avoid negative revelations. Thus, the desire to harm the United States does not necessarily motivate a spy.

Likewise, disclosures to the media may not be motivated by a desire to inform public debate. For example, Morison's disclosure to the defense magazine was allegedly motivated by a desire to gain employment with the magazine.[240] Recent indictments further illuminate the uncertainty in individuals' motivations. The rising occurrence of disclosures in social media, as exemplified by Teixeira, introduces the desire for social clout as a motivating cause.[241] Trump's alleged "cavalier" disclosure of nuclear submarine capabilities to an Australian businessman supports the same conclusion.[242] The United States has updated its strategies to recruit foreign agents to exploit these social dynamics and feed on a potential recruit's desire

237. *See* Ellis Cose, *The Short Life and Curious Death of Free Speech in America*, AM. C.L. UNION (Sept. 21, 2020), https://www.aclu.org/news/civil-liberties/the-short-life-and-curious-death-of-free-speech-in-america (excerpting ELLIS COSE, THE SHORT LIFE AND CURIOUS DEATH OF FREE SPEECH IN AMERICA (2020)); *see also* David Hudson, *Counterspeech Doctrine*, FREE SPEECH CTR. (July 2, 2024), https://firstamendment.mtsu.edu/article/counterspeech-doctrine/.

238. CIA psychologist Dr. Ursula Wilder studies the motivations of both spies and leakers, concluding both often exhibit similar traits. Ursula Wilder, *The Psychology of Espionage and Leaking in the Digital Age*, STUD. INTEL., June 2017, at 1, 1–4.

239. These approaches are aptly summarized in the mnemonic M.I.C.E. (money, ideology, compromise, ego). *See* Randy Burkett, *An Alternative Framework for Agent Recruitment: From MICE to RASCLS*, STUD. INTEL., March 2013, at 7, 7.

240. *See* Eric Setzekorn, *The Contemporary Utility of 1930s Counterintelligence Prosecution Under the United States Espionage Act*, 29 INT'L J. INTEL. & COUNTERINTELLIGENCE 545, 557 (2016).

241. *See* Askonas & DiResta, *supra* note 200.

242. *See* Alan Feuer, Ben Protess, Maggie Haberman & Jonathan Swan, *Trump Said To Have Revealed Nuclear Submarine Secrets to Australian Businessman*, N.Y. TIMES (Oct. 5, 2023), https://www.nytimes.com/2023/10/05/us/politics/trump-nuclear-submarine-classified-documents.html.

to be liked.[243] The reality of an individual's motivations to disclose protected information precludes a clear distinction between spies and leakers.

Amending the Act to offer an affirmative "public interest" defense[244] would render the Act toothless. This affirmative defense threatens to swallow mens rea requirements entirely because "[m]ost leakers can plausibly claim that at least one of their motives was altruistic, and it may be impossible to establish with any certainty whether a defendant's professed motive is sincerely held."[245] Such a defense could effectively create a loophole where spies could immunize their actions by arguing good intent. Even if such insincere defenses were always uncovered, finding liability only after demonstrating a specific intent to harm the U.S. or excusing liability after establishing goodwill is misaligned with the actual motivations of spies and leakers.

Furthermore, considering the Act's general purpose of deterring acts harmful to the U.S., the motive for a disclosure does not alter the harm of the disclosure. Rather than probing an individual's subjective intent, objective intent may be inferred from the action. Such an objective standard currently operates under the Act by defining the type of information prohibited from disclosure to be information "that would be objectively useful for a foreign country."[246] For a government employee turned spy or leaker, the objective standard is especially pronounced where obtaining a security clearance and access to classified information requires training and acknowledgement of the consequences for unauthorized disclosure. This intimate knowledge of information's classification provides clear evidence of knowledge of a disclosure's potential harm.[247] Although numerous criminal laws require subjective intent,[248] special considerations of Espionage Act prosecutions support a more streamlined analysis achieved with the current mens rea standards. Therefore, attempting to absolve liability for alleged good intentions misunderstands the actual motivations of spies and leakers and undermines the Act's purpose.

3. Balancing Harm to National Security with Benefit to Public Debate

Lastly, adopting a balancing test to determine whether the benefit to public debate outweighs the harm to national security[249] would establish an unrealistic

---

243. *See* Burkett, *supra* note 239, at 12–13 (discussing "Liking" as a principle of the updated approach to recruitment, noting "[f]lattery is highly recommended, for virtually everyone enjoys being praised").

244. *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.

245. Ryan, *supra* note 156, at 74; *see also* Papandrea, *National Security Information*, *supra* note 127, at 1436 ("One problem with focusing on the purpose—or motivation—for disclosures is that leakers, as well as spies, can have any number of reasons for their disclosures that have nothing to do with a desire to harm the United States . . . .").

246. *See* Papandrea, *National Security Information*, *supra* note 127, at 1408.

247. *See* United States v. Kiriakou, 898 F. Supp. 2d 921, 925 (E.D. Va. 2012) (noting cleared government employees "could appreciate the significance of the information . . . allegedly disclosed").

248. *See* Papandrea, *Leaker Traitor*, *supra* note 140, at 540 (noting other criminal statutes require intent, but acknowledging "determining intent can be tricky").

249. *See* Takefman, *supra* note 162, at 900.

inquiry. Courts do not currently perform such balancing, and no defendant has been acquitted on the reasoning that the benefit of the disclosure outweighs the harm.[250] Even so, imposing a balancing test is a common proposal to reform the Act. One scholar essentializes this balancing test to simply ask: "Is it news worthy? Or is it spy worthy?"[251] However, this simplified classification is unrealistic because information useful for informed public debate is often valuable to adversarial spies.[252] The difficulty of balancing harm and benefit is especially pronounced with classified information. As mentioned previously, the precise harms are often not immediately known and then often only within classified spheres. Furthermore, even the benefit to public debate may be unclear where leaks may be biased or provide an incomplete picture.[253] This skew in public debate is often unanswered because the government is unlikely to release further information necessary for a truly informed debate.

A more fundamental issue with a balancing test is the displacement of national security decision-making. The President is the "sole organ" in foreign affairs and the Supreme Court recognizes the necessity of secrecy in the exercise of this power.[254] The President achieves this secrecy via the classification system. The Executive Branch classifies information based on the degree of harm resulting from disclosure.[255] Thus, the very nature of the classification system requires the Executive to balance free speech with national security.[256] Adopting a balancing test to determine liability under the Espionage Act shifts the onus of this decision-making away from the President to government employees, journalists, or the judiciary. Accurately assessing this balance requires a holistic understanding of foreign policy, which only the highest executive-branch officials possess. Even seemingly innocuous information may provide adversaries a crucial piece of information, having far worse harms than the content suggests.[257] Thus, only the President and top executive officials—not individual

250. *See* MULLIGAN & ELSEA, *supra* note 95, at 14.

251. Mark Norris, *Bad "Leaker" or Good "Whistleblower"?—A Test*, 64 CASE W. RES. L. REV. 693, 706 (2013).

252. *See* Papandrea, *National Security Information*, *supra* note 127, at 1435–36 ("Information about government misconduct that is illegal or conduct likely to be regarded by the public as excessive may give the targets of these programs the opportunity to avoid surveillance, but the disclosures will spur public debate about the programs.").

253. *See* Papandrea, *Leaker Traitor*, *supra* note 140, at 480–81.

254. *See* United States v. Curtiss-Wright Export Corp., 299 U.S. 304, 320 (1936). ("He has his confidential sources of information. . . . Secrecy in respect of information gathered by them may be highly necessary, and the premature disclosure of it productive of harmful results.").

255. The levels of classification are described *supra* note 137.

256. For a comprehensive discussion of Presidential power in this arena, see generally Edgar & Schmidt, *supra* note 202.

257. *See id.* at 400 ("There is also the ever present possibility that an employee may not realize why certain seemingly insignificant information is important for security purposes."); Greg Miller, *CIA's Secret Agents Hide Under a Variety of Covers*, SEATTLE TIMES (July 25, 2005, 12:00 AM), https://www.seattletimes.com/nation-world/cias-secret-agents-hide-under-a-variety-of-covers/ (Former CIA case officer noting, "Cover is a mosaic, it's a puzzle. . . . Every piece is important [to protect] because you don't know which pieces the bad guys are missing.").

employees,[258] journalists,[259] or the courts[260]—are equipped to make the determinations necessary to protect national security.

Proposals designed to differentiate treatment between spies and leakers diminish the Espionage Act's deterrent effect. In addition to the practical untenability of proving subjective intent or balancing harms and benefits, these ex post determinations reduce the certainty of prosecution under the Act.[261] Deterrence requires certainty, but determining liability *after* the disclosure does nothing to prevent the harm to national security. Thus, even if there were principled legal distinctions between spies and leakers, they would be unwise to enact. Instead, supporting the Espionage Act and its application to spies and leakers is essential to deter disclosures harmful to national security. Where domestic law is the vehicle to deter international acts of espionage, this deterrence has domestic and international consequences.

IV. REFORMS FOR A COHERENT, LEGITIMATE LEGAL REGIME

The Espionage Act is essential to criminalize actions harmful to U.S. national security and must necessarily partially restrict the ability of citizens to speak freely. This tension exemplifies the long struggle to balance national security with constitutional rights.[262]

National security is only as good as the values it secures. Justice Warren noted, "[i]t would indeed be ironic if, in the name of national defense, we would sanction the subversion of one of those liberties . . . which makes the defense of the Nation worthwhile."[263] Yet, the Constitution "is not a suicide pact."[264] Adopting the most

---

258. *See* Ryan, *supra* note 156, at 74 ("A policy of tolerating leaks with purportedly worthy motives would effectively permit private individuals to usurp the authority of Congress and the President to make critical national security decisions on behalf of the country.").

259. *See* Freivogel, *supra* note 161, at 117 ("If journalists are not specially qualified to evaluate national security information and do not have security clearances, what makes them qualified to make the national security judgment that is part of the calculus of determining if society will be better off if the secret is disclosed?").

260. The Judiciary itself notes its lack of competence to effectively adjudicate questions of foreign policy. *See* Chicago & Southern Air Lines, Inc. v. Waterman S.S. Corp., 333 U.S. 103, 111 (1948) (noting foreign policy decisions are "of a kind for which the Judiciary has neither aptitude, facilities nor responsibility and have long been held to belong in the domain of political power not subject to judicial intrusion or inquiry").

261. *See* Stone, *supra* note 201, at 192 (commenting that an approach where the First Amendment protects only speech where value outweighs harm "would put the courts in an extremely awkward position and effectively would convert the First Amendment into a constitutional Freedom of Information Act").

262. *See* Edgar & Schmidt, *supra* note 103, at 939. Edgar & Schmidt explain:

> Congress, however, has grappled with the problems of accommodating secrecy and public speech on at least five occasions since 1911. In each instance, the legislative debates have focused on the problem of how to protect military secrets from spies without promulgating broad prohibitions that would jeopardize the legitimate efforts of citizens to seek information and express views concerning national security.

Id.

263. United States v. Robel, 389 U.S. 258, 264 (1967).

264. Kennedy v. Mendoza-Martinez, 372 U.S. 144, 160 (1963).

effective deterrent to protect national security would impermissibly infringe free speech principles central to this country.[265] In contrast, adopting the most expansive interpretation of freedom of speech would sanction the release of an impermissible amount of sensitive information, greatly damaging national security.[266] Thus, the solution is to strike a balance between these competing values to ensure security for the ideals held most dear.[267]

The Espionage Act in its current operation strikes this balance. As discussed above, the statute, caselaw, and prosecutorial decisions generally uphold this balance. The Espionage Act is broad enough to provide essential deterrence for both spies and leakers. Caselaw emphasizes that the harm of the disclosure, not the intent or potential public benefit, matters most. Furthermore, a prosecution has never been brought against a member of the media solely for passively publishing information.[268] This balance is practical. It vigorously prosecutes disclosures to deter the release of information harmful to national security, yet it protects the press's subsequent publication of information, which facilitates an informed electorate.[269]

Considering the fundamental balance between the competing interests, any reform of the Espionage Act should target clarification of the Act's scope and

---

265. *See* Edgar & Schmidt, *supra* note 202, at 401 ("[C]riminalizing all publication of secret facts about the government, whether or not related to national security matters, must be held unconstitutional unless we are willing to abandon large portions of our first amendment jurisprudence.").

266. *See* United States v. Rosen, 445 F. Supp. 2d 602, 629 (E.D. Va. 2006) ("Defendants' First Amendment challenge exposes the inherent tension between the government transparency so essential to a democratic society and the government's equally compelling need to protect information from disclosure information that could be used by those who wish this nation harm.").

267. *See id*. The *Rosen* court stated:

> [I]t is important to bear in mind that the question to be resolved here is not whether § 793 is the optimal resolution of this tension [between free speech and national security], but whether Congress, in passing this statute, has struck a balance between these competing interests that falls within the range of constitutionally permissible outcomes.

Id.

268. *See* Stone, *supra* note 201, at 213 ("The United States has made it through more than two hundred years without ever finding it necessary to prosecute a journalist for soliciting a public employee to disclose confidential national security information.").

269. Edgar & Schmidt, *supra* note 103, at 1037. Edgar and Schmidt maintain:

> We might well adopt a system which protects all acts in the publication process but makes criminal the initial revelation by the government employee. Such a system would be a rational, if a bit uneasy, compromise of the competing values of secrecy and executive branch loyalty, on one side, and freedom of speech on the other.

Id.; *see also* Stone, *supra* note 201, at 200. Stone explains:

> The solution, which has stood us in good stead for more than two centuries, is to reconcile the conflicting values of secrecy and accountability by guaranteeing both a strong authority of the government to prohibit leaks and an expansive right of the press to publish them. This solution may seem awkward in theory and unruly in practice, but it has withstood the test of time.

Id.

improvement of public perceptions of the Act's legitimacy. Because of the Act's broad language, this Part argues that the Act should better reflect that mens rea is an objective intent standard and does not wade into murky determinations of the discloser's subjective intent. This Part also argues that the Act should codify protections for the press passively receiving information. However, initiating reforms before reaching public consensus that the Act properly applies to both spies and leakers threatens to disrupt the delicate balance between national security and constitutional rights, as well as degrade the Act's deterrent effect. Instead, this Part argues that Espionage Act prosecutions should more actively attempt to promote public perceptions of the Act's legitimacy by emphasizing the harm to national security and avoiding any appearance of political motivation.

A. Clarifying the Espionage Act's Operation

As argued here, the substance of the Espionage Act strikes the correct balance between national security and constitutional rights. However, the express terms of the Espionage Act are "murky,"[270] "incomprehensible,"[271] and "so sweeping as to be absurd,"[272] resulting in sometimes "tortured" analysis to reconcile the statute's terms with legislative intent and caselaw.[273] Amending the Act to clarify its terms and operation would benefit practitioners, legal scholars, and the public. However, any reform to the language of the Act must be assessed in relation to both spies and leakers to ensure effective deterrence. Specifically beneficial would be amending the language to clarify the mens rea requirements—particularly to specify an objective, not subjective standard—and to codify press protections for essential newsgathering activities.

The Act should specify press protections for passive receipt of information in legitimate newsgathering activities. As discussed above, the tension between newsgathering and receiving classified information has yet to be tested. This uncertainty and the threat of prosecution represents a "loaded gun pointed at newspapers and reporters."[274] However, in October 2022, the Department of Justice resolved this tension with updated regulations for charging members of the press.[275] The regulations define newsgathering to include the receipt of classified information.[276] This protection preserves the passive receipt of information without sanctioning the active participation in illegal disclosure. Furthermore, the regulations exempt foreign powers and agents,[277] which preserves the Espionage Act's application to

270. Edgar & Schmidt, *supra* note 202, at 394.

271. *Id.* at 393 ("The espionage statutes are incomprehensible if read according to the conventions of legal analysis of text, while paying fair attention to legislative history.").

272. Edgar & Schmidt, *supra* note 103, at 1032.

273. For an extensive recounting of legislative intent and the Act's language, see generally *id.* at 936–42.

274. *See id.* at 936.

275. *See* Dep't of Just., 28 C.F.R. pt. 50 (2022) (issuing a policy regarding obtaining information from news media).

276. 28 C.F.R. § 50.10(b)(2)(ii)(A) (2022).

277. *Id.* § 50.10(b)(3)(i) (2022).

foreign handlers receiving protected information. Amending the Espionage Act to include these regulations would codify press protections, alleviating some of the most strident critiques of the Act.

Although these suggested reforms merely codify current understanding and practices of the Act, attempting to amend the language of the statute to clearly incorporate these reforms is ill-advised until there exists consensus that espionage includes both classic spies and leakers. Proposed amendments to the Espionage Act often operate at the extremes: seeking to exempt leakers[278] or strictly punish every disclosure.[279] The former will hinder the ability to prevent harmful disclosures. The latter unduly restricts free speech. Revisiting the law with such a disparity in the Act's desired function threatens to incorporate language that dilutes the law's essential deterrent effect or invites such vigorous opposition that its very legitimacy is undermined. Until there is consensus on the importance of the Espionage Act's application to spies and leakers and its inapplicability to legitimate newsgathering, the Act should remain untouched.

B. Improving Legitimacy

Owing to an unsavory history of political prosecutions and a general misunderstanding of the practice of espionage, broad swaths of the public view the Espionage Act as illegitimate.[280] Rehabilitating the Act's public image is essential to maintaining its deterrent effect. A reasonable exercise of prosecutorial discretion is necessary to improve the Act's legitimacy.[281] Prosecutors must reinforce the Act's legitimacy by emphasizing the resulting harm, bolstering its deterrent effect, targeting qualifying actions regardless of the defendant's identity, and adhering to stringent ethical standards.

Some prosecutions damage the Act's legitimacy by the seeming inability for the disclosure to harm national security. The Espionage Act's broad language covers every case from Robert Hanssen to a stray document unintentionally taken home in a briefcase.[282] For example, one of the documents at the center of Thomas Drake's prosecution involved a schedule of meetings formally categorized as Unclassified/For Official Use Only.[283] Without knowing the full extent of national

278. *See, e.g.*, H.R. Rules Comm., Proposed Amendment to National Defense Authorization Act by Rep. Rashida Tlaib (June 30, 2022), https://amendments-rules.house.gov/amendments/TLAIB_091_xml220705104842068.pdf (proposing multiple revisions to include revising 18 U.S.C. § 793 to require "specific intent to injure the United States" and providing an affirmative defense if public disclosure is made for the purpose of disclosing violations of laws, rules, or regulations or gross mismanagement and waste); H.R. Rules Comm., Proposed Rule to Protect Brave Whistleblowers Act of 2020 by Rep. Tulsi Gabbard (Sept. 30, 2020), https://www.govtrack.us/congress/bills/116/hr8452/text (same).

279. *See* MULLIGAN & ELSEA, *supra* note 95, at 30.

280. *See* Ryan, *supra* note 156, at 75–76.

281. *See id.* at 62–63, 80.

282. *See, e.g.*, United States v. Roller, 42 M.J. 264, 264–65 (C.A.A.F. 1995) (finding military member guilty under 18 U.S.C. § 793(f) for taking a classified document home in a gym bag and failing to report mistake).

283. *See* Takefman, *supra* note 162, at 917.

security considerations concerning this schedule, the public may believe this information poses minimal harm to national security and reasonably conclude that the prosecution is meritless.[284] Like the boy who cried wolf, citing espionage for *any* piece of classified information undermines legitimate invocation of harm when it truly matters. The government need not prove harm, but it must defend its prosecutions to garner public acceptance of their legitimacy.

However, a prosecution's deterrent effect, not simply the amount of harm alleged, should be a requirement for all cases brought under the Espionage Act. A low-level disclosure, when viewed individually, may not appear to warrant indictment under the Act. However, in the aggregate, information gleaned from collecting snippets of seemingly innocuous information can cause tangible harm. Thus, declining to prosecute lower-level violations of the Espionage Act invites national security harm in the form of death by a thousand cuts. Communicating the rationale behind such prosecutions is essential for the Act to remain an effective and legitimate deterrent.

Prosecutors must also adopt guidelines to address the differential application of the Act based on the potential defendant's stature. Many leaks originate from high-level government officials.[285] Prosecuting these high-level officials in addition to low- and mid-level employees will undermine critics' arguments that the Act places some individuals above the law.[286]

Finally, prosecutors must exhibit the highest ethical standards. Daniel Ellsberg's prosecution ended in mistrial because prosecutors illegally wiretapped, ordered a break-in of Ellsberg's psychiatrist's office, and destroyed evidence.[287] This misconduct destroyed the prosecution's credibility, undermining the asserted harm of the leak. To critics, this case now serves as an exemplar of illegitimacy, tainting all future prosecutions. Rehabilitating the legitimacy of the Espionage Act requires that every prosecution rests on the validity of the Act itself and does not resort to dirty tricks.

Because punishment and deterrence under this Act is essential to protect information vital to this country's security, the Act's continued efficacy depends on acceptance of the Act's purpose. To improve the Act's legitimacy and effective operation, the Act must be seen as preserving the delicate balancing act between

---

284. *See id.* at 899–900 (noting the judge's general distaste for the government's conduct throughout the Drake prosecution); *see also* Jane Mayer, *The Secret Sharer*, NEW YORKER (May 23, 2011), https://www.newyorker.com/magazine/2011/05/23/the-secret-sharer.

285. *See* Papandrea, *Leaker Traitor*, *supra* note 140, at 464 ("[T]he ship of state is the only ship that leaks from the top." (footnote omitted)).

286. *See* Ryan, *supra* note 156, at 75–76. ("Prosecutors should also consider the perceptions of illegitimacy and unfairness associated with an enforcement approach that imposes harsh criminal punishment on lower-level employees while shielding high-ranking officials."); *see also* Papandrea, *Leaker Traitor*, *supra* note 140, at 462 (citing research with CIA officials indicating the agency considers "rank, message, internal politics and whim," when enforcing secrecy provisions).

287. *See* MULLIGAN & ELSEA, *supra* note 95, at 15.

national security and constitutional rights, which can be accomplished by codifying constitutional protections and pursuing principled and ethical prosecutions.

CONCLUSION

The Espionage Act is a drastically important, yet wildly misunderstood law. It operates at the confluence of international and domestic law and implicates both intelligence operations required for national security and First Amendment protections essential to the fabric of this nation. This Note seeks to unite these facets to conceptualize a holistic picture of the Espionage Act. The Act is essential to deter and punish those who engage in the unauthorized disclosure of sensitive information relating to national security—those who engage in espionage.

Although leaks of classified information have triggered important government reforms, there exists no principled legal distinction to punish a spy yet exonerate a leaker. The *crime* of espionage must apply uniformly to the acts which cause harm. The rule of law requires this. However, there may indeed be instances where the need to disclose government wrongdoing overshadows potential harm to national security. This determination, however, must be a *moral* decision, not a *legal* one.[288] For some, the choice to disclose such information "might sometimes be necessary, but it should not be easy,"[289] and the discloser must accept full responsibility and all attendant consequences.[290] This choice must also be rare, which requires reforms to improve the potency of classified designations and restrict access to sensitive information to only those who are most deserving.[291]

A fundamental, yet inherent flaw in the Espionage Act's operation is the inability for the government to adequately convey to the public the importance of secrecy to national security. National security failures are advertised publicly, while successes are celebrated in secret. This Note hopes to prompt discussions that adopt simultaneous appreciation of the complex, dire decisions made every day to secure this nation and gratitude for the liberties and protections that make this country worth securing.

---

288. *See* Vladeck, *supra* note 215, at 1535.

289. *See* Mary DeRosa, *National Security Lawyering: The Best View of the Law as a Regulative Ideal*, 31 GEO. J. LEGAL ETHICS 277, 303 (2018) (discussing permission structures created by relaxing standards within national security lawyering).

290. *See* Freivogel, *supra* note 161, at 97 ("[Leakers] need to face the fact that they are engaging in an act of civil disobedience for which they must accept the legal consequences.").

291. Such reform requires combating the rampant over-classification of information and creating stricter vetting procedures for individuals obtaining and keeping security clearances. As an example, the National Geospatial-Intelligence Agency revamped its classification procedures in an initiative to build "higher walls around fewer secrets." *See* Bruce, *supra* note 100.