NATIONAL SECURITY INFORMATION DISCLOSURES AND THE ROLE OF INTENT

MARY-ROSE PAPANDREA*

TABLE OF CONTENTS

* Professor of Law, Boston College Law School. I would like to thank David Ardia, Elizabeth Ludwin King, Heidi Kitrosser, and all the participants at the *William & Mary Law Review* Symposium on "The Contemporary First Amendment," as well as the participants at a faculty workshop at The University of North Carolina School of Law. I am also grateful for a summer research grant from the Patricia and John McHale Fund for Faculty Research and the research assistance of John Giampa.

INTRODUCTION

In the public discourse, the perceived intent of those who disclose national security information without authorization plays an important role in whether they are labeled as heroes or traitors.[1] Should it matter whether Chelsea (formerly Bradley) Manning leaked government information to WikiLeaks knowing that our enemies might benefit from the information? Is it relevant that Edward Snowden believed—or that a reasonable person would believe—that the top-secret government surveillance programs he revealed were illegal, or that the public value in knowing about these programs outweighed any risk of harm to national security? This Article examines whether intent—and what kind of intent— should matter in defining crimes related to the disclosure of national security information and concludes that it should, both as a matter of public policy and as a matter of constitutional law.

Although strict liability for the unauthorized collection and dissemination of all defense-related information might be the safest way to protect our nation's security,[2] such an approach would be inconsistent with our basic commitment to an informed democracy. The difficulty is in balancing the competing interests at stake. Incorporating mens rea requirements is a potentially useful way to strike the appropriate balance. Indeed, mens rea requirements are used throughout criminal law to differentiate among actors based on their moral blameworthiness and already play a very important role in defining and limiting criminal liability in this area. The current statutory regime—as convoluted and confusing as it is—treats the transmission of national security information with the intent to aid the enemy or a foreign government much more severely

1. *See, e.g.*, Suzanna Andrews et al., *The Snowden Saga: A Shadowland of Secrets and Light*, VANITY FAIR (May 2014), http://www.vanityfair.com/news/politics/ 2014/05/edward-snowden-politics-interview [http://perma.cc/6JRG-HFZA] ("Whether hero or traitor, former National Security Agency contractor Edward Snowden is the most important whistle-blower of modern times."). For a more extensive discussion of this "name game," see Mary-Rose Papandrea, *Leaker Traitor Whistleblower Spy: National Security Leaks and the First Amendment*, 94 B.U. L. REV. 449, 450-53 (2014).

2. Harold Edgar & Benno C. Schmidt, Jr., *The Espionage Statutes and the Publication of Defense Information*, 73 COLUM. L. REV. 929, 1083 (1973).

than other types of unauthorized disclosures.[3] As the U.S. Supreme Court has explicitly recognized, "innocence of intention will defeat a charge even of treason."[4] Disclosures made with "bad" intent—for example, to aid one of our enemies or to harm the United States—are entitled to greater moral condemnation and punishment.[5]

It is less clear whether the First Amendment requires any consideration of intent when determining which disclosures of national security information can be punished. Surprisingly, the role of intent in the Court's First Amendment jurisprudence has received little scholarly attention.[6] Even less explored is the more specific question of the role of intent with respect to First Amendment protection for the disclosure and publication of national security

---

3. 18 U.S.C. § 794(a)-(b) (2012) (authorizing up to life in prison and the death penalty for those who gather or deliver national security information to any foreign government or enemy "with the intent or reason to believe" that it "is to be used to the injury of the United States or advantage of a foreign nation").

4. Morissette v. United States, 342 U.S. 246, 262 n.21 (1952) (citing Haupt v. United States, 330 U.S. 631 (1947); Cramer v. United States, 325 U.S. 1 (1945)); *id.* at 265 ("[T]reason—the one crime deemed grave enough for definition in our Constitution itself—requires not only the duly witnessed overt act of aid and comfort to the enemy but also the mental element of disloyalty or adherence to the enemy.").

5. Government officials frequently argue that motivation is irrelevant because information disclosed with the intent of informing public debate will end up in our enemies hands, causing the same harm as information delivered directly to our enemies. See Edgar & Schmidt, Jr., *supra* note 2, at 942; *see also* Papandrea, *supra* note 1, at 450 n.2-3 (summarizing various government statements suggesting that any leak to the press is the equivalent of aiding the enemy).

6. *See* Larry Alexander, *Free Speech and Speaker's Intent*, 12 CONST. COMMENT. 21, 21-22 (1995) (arguing against using intent in First Amendment jurisprudence because no matter what the author intended, audiences will receive it differently); Larry Alexander, *Low Value Speech*, 83 NW. U. L. REV. 547, 548, 552 n.19 (1989) (stating that the problem with using the speaker's intent is that the value of speech is derived from the audience's interpretation of the speech, not the speaker's intent); Frederick Schauer, *Intentions, Conventions, and the First Amendment: The Case of Cross-Burning*, 2003 SUP. CT. REV. 197, 199 ("[Q]uestions about the relevance of speaker's intent, although pervasively important in free speech analysis, have rarely surfaced explicitly in either the case law or the literature."). *But see* Leslie Kendrick, *Free Speech and Guilty Minds*, 114 COLUM. L. REV. 1255, 1255-56 (2014) (arguing that First Amendment law considers the speaker's intent and demonstrating how and why the speaker's intent matters). It is likely that more scholars will focus on the role of intent in determining the scope of First Amendment protection now that the U.S. Supreme Court will be deciding whether a defendant must subjectively intend for his communication to be perceived as intimidating in order for his speech to constitute a "true threat," an unprotected category of speech. *See* United States v. Elonis, 730 F.3d 321, 324 (3d Cir. 2013), *cert. granted*, 134 S. Ct. 2819 (2014).

information.[7] Although many scholars have suggested that intent should play a role in the badly needed revision of the Espionage Act and related statutes, the literature lacks a vigorous study of why intent should matter, what the relevant intent requirements should be, and whether any of these requirements are constitutionally required.[8] This Article focuses on these questions.

---

7. The best analysis of the culpability standards in the current federal statutes relating to the collection, retention, and dissemination of national security information is Harold Edgar and Benno Schmidt's seminal article on the Espionage Act statutes. *See* Edgar & Schmidt, Jr., *supra* note 2. Because they conclude that "the central issues are legislative," however, this Article does not focus on whether the First Amendment requires any particular culpability standards. *Id.* at 930 ("The first amendment provides restraints against grossly sweeping prohibitions, but it does not, we believe, deprive Congress of considerable latitude in reconciling the conflict between basic values of speech and security."); *id.* at 1044-46 (arguing that construing § 793(d) and (e) of the Espionage Act to take the defendant's motives into account would help avoid a potential "[c]onstitutional dilemma[ ]" of criminalizing speech protected under the First Amendment). That said, I am tremendously grateful for the many insights they offer throughout their article regarding the proper balance between protecting our national security and securing free debate.

8. *See*, *e.g.*, *Espionage Act and the Legal and Constitutional Issues Raised by WikiLeaks: Hearing Before the H. Comm. On the Judiciary*, 111th Cong. 66-69 (2010) [hereinafter *Espionage Act Hearing*] (statement of Stephen I. Vladeck, Professor of Law, American University Washington College of Law), *available at* http://perma.cc/6X6X-JS7U (suggesting that Congress add to the Espionage Act "a clear and precise specific intent requirement that constrains the scope of the Espionage Act to cases where the defendant specifically intends the disclosure to harm national security and/or to benefit a foreign power," and a separate, lesser crime for other disclosures with "the availability of any number of affirmative defenses that the disclosure was in good faith; that the information was improperly classified; that the information was already in the public domain; and/or that the public good resulting from the disclosure outweighs the potential harm to national security"); Patricia Bellia, *WikiLeaks and the Institutional Framework for National Security Disclosures*, 121 YALE L.J. 1448, 1523 (2012) (suggesting that Congress "distinguish between disclosures undertaken with intent to harm the United States or benefit a foreign nation, disclosures undertaken with reckless disregard for this risk, and disclosures undertaken in bad faith and where the leaker knew or had reason to know that disclosure would pose significant national security risks"); Yochai Benkler, *A Public Accountability Defense for National Security Leakers and Whistleblowers*, 8 HARV. L. & POL'Y REV. 281, 305 (2014) (arguing for a public accountability defense requiring a defendant to demonstrate an objectively reasonable belief that his disclosure would expose "a substantial violation of law or systemic error, incompetence, or malfeasance" and suggesting the subjective motivation is irrelevant, as well as any ultimate determination regarding the legality of the disclosed government activities); Heidi Kitrosser, *Classified Information Leaks and Free Speech*, 2008 U. ILL. L. REV. 881, 928 (arguing it is essential to "preserve[ ]" the intent requirement in cases against government outsiders because it "safeguards against punishments based on mere policy disagreements over secrecy and openness"); Heidi Kitrosser, *Free Speech Aboard the Leaky Ship of State: Calibrating First Amendment Protections for Leakers of Classified information*, 6 J. NAT'L SEC. L. & POL'Y 409, 441 (2013) (arguing that the First Amendment protects leakers from severe sanctions when they had an "objec-

Part I surveys the current role of intent in the notoriously convoluted Espionage Act and related statutes. This overview of Congress's struggle to protect the freedom of speech while punishing spies and others who harm our national security interests is useful on several levels. These statutes as well as their legislative histories demonstrate that the idea of using intent standards to distinguish between speech that should be protected and speech deserving of punishment is hardly a new idea. As with many other federal statutes, however, Congress's use of intent standards in the existing statutory framework is clumsy and vague. As a result, courts interpreting these laws disagree about what level of culpability is required. Furthermore, these statutes illustrate the common problem of using intent standards to draw distinctions among acts that may cause similar harms.[9] At the same time, however, Congress's

---

tively *reasonable* basis to believe that the public interest in disclosure outweighed identifiable national security harms" and from less severe sanctions when leakers have an "objectively *substantial* basis to believe that the public interest in disclosure outweighed identifiable national security harms"); David McCraw & Stephen Gikow, *The End to an Unspoken Bargain?*, 48 Harv. C.R.-C.L. L. Rev. 473 (2013) ("There is ... a case to be made that intent should matter—those who publish with knowing intent to harm can be distinguished from those who publish with a good-faith belief that they are advancing public knowledge and debate."); Derigan A. Silver, *National Security and the Press: The Government's Ability to Prosecute Journalists for the Possession or Publication of National Security Information*, 13 COMM. L. & POL'Y 447, 483 (2008) (calling on Congress to amend the Espionage Act statutes "to limit prosecution to instances when there is evidence of intent to harm the United States"); Geoffrey Stone, *Government Security v. Freedom of the Press*, 1 HARV. L. & POL'Y REV. 185, 196 (2007) (arguing that the First Amendment offers no protection to government employees who disclose information about a national security program the employee "reasonably but *wrongly* believed to be unlawful"); Christina E. Wells, *Contextualizing Disclosure's Effects: WikiLeaks, Balancing, and the First Amendment*, 97 IOWA L. REV. BULL. 51, 63 (2012), http://ilr.law.uiowa.edu/files/ilr.law.uiowa.edu/files/ILRB_97_Wells.pdf [http://perma.cc/SSP9-KRB9] (arguing for a revised "judicial test" that "require[s] strong evidentiary showings, clear intent requirements, and other protections to ensure that balancing does not routinely work to the detriment of those who disclose information for nonespionage purposes"); *see also* Candice Kines, Note, *Aiding the Enemy or Promoting Democracy? Defining the Rights of Journalists and Whistleblowers*, 116 W. VA. L. REV. 735, 778-79 (2013) (arguing for the amendment of the Espionage Act to protect disclosures of national security made with the good-faith intention to promote public awareness of an act "perceived to be illegal or unjust"); Eric A. Posner, *Before You Reboot the NSA, Think About This*, NEW REPUBLIC (Nov. 6, 2013), http://www.newrepublic.com/article/115291/rahul-sagars-secret-leaks-reviewed-eric-posner [http://perma.cc/4R5F-2BKN] (stating that "nearly all members of the intelligentsia—journalists, pundits, university professors" believe that "[w]histle-blowers should not be prosecuted when they mean well and disclose wrongdoing").

9. *See* Note, *Mens Rea in Federal Criminal Law*, 111 HARV. L. REV. 2402, 2402 (1998) (lamenting the "confused and inconsistent ad hoc approach" of courts interpreting mens rea

persistentuse of intent requirements to determine which disclosures are criminalized and which ones are not is instructive, offering useful lines of inquiry regarding how mens rea requirements could be used in this context.

Part II examines the often controversial role of intent in the U.S. Supreme Court's First Amendment jurisprudence and concludes that even if Congress declines to incorporate intent into the statutory framework for national security information disclosures, such intent standards may be constitutionally required. Mens rea standards are an extraordinarily useful means of distinguishing between espionage, which can be said to serve no constructive purpose, and leaks, which often make meaningful contributions to public debate. In addition, intent standards can be used not just as a means of demarking protected speech and unprotected speech but also as way of determining the severity of the crime. Furthermore, culpability standards offer a particularly promising means of dealing with the problem of "dual use" speech, which is speech that can be either helpful or harmful. The unauthorized disclosures of national security information fall within this category because they can both make a meaningful contribution to the public debate and threaten our national security.

Part III addresses the likely objections to the use of intent standards to draw distinctions between protected and unprotected disclosures. Among other things, this portion of the Article explains that in determining a speaker's intent, courts are not required to

---

in federal criminal statutes) (citation omitted). The Court has particularly struggled to interpret federal statutes that contain no mens rea requirements at all, especially when the crimes are not public welfare offenses and the statutorily authorized punishment is severe. In several cases, the Court has read mens rea requirements into federal statutes in order to avoid criminalizing "apparently innocent conduct." *See, e.g.*, United States v. X-Citement Video, Inc., 513 U.S. 64, 65-66, 68-69 (1994) (extending a mens rea requirement to additional elements of the criminal statute despite the statute's plain textual reading); Staples v. United States, 511 U.S. 600, 602, 605-06 (1994) (incorporating a mens rea requirement into the federal statute penalizing the failure to register certain types of firearms); Liparota v. United States, 471 U.S. 419 (1985) (interpreting a federal criminal law relating to misuse of food stamps); Morissette v. United States, 342 U.S. 246 (1952) (interpreting a federal embezzlement statute). *But see* United States v. Balint, 258 U.S. 250, 254 (1922) (declining to read a mens rea requirement into a federal drug law provision after concluding that Congress had "weighed the possible injustice of subjecting an innocent seller to a penalty against the evil of exposing innocent purchasers to danger from the drug, and concluded that the latter was the result preferably to be avoided").

accept a defendant's potentially self-serving explanations for his speech, but instead can consider a variety of contextual clues to determine the legitimacy of those assertions.

Before I begin, a few caveats are in order. This Article rests on a number of background assumptions that some readers might regard as controversial. To begin, this Article takes it as a given that the overclassification of national security information is rampant, and as a result the classification status of a document should not be absolutely determinative regarding the value of the information or the need for secrecy. As Judge Skelly Wright said in his dissent from the D.C. Circuit's decision to grant the government's request for a prior restraint in *United States v. Washington Post Co.*, "To allow a government to suppress free speech simply through a system of bureaucratic classification would sell our heritage, far, far too cheaply."[10] Furthermore, this Article takes as a given that leaks of classified information are an essential part of our democracy. In some ways, the resulting "game of leaks" serves both the government, which uses leaks to control the flow of information for its own purposes, and the press, which may benefit financially and otherwise from its ability to expose and decipher national security secrets. In my prior work,[11] I have explored the various problems with the classification system, the lack of effective whistleblower protections for national security employees, the symbiotic relationship between the press and the executive branch, and the role of leaks as an effective check on the political branches; I do not set out to prove them all here again.

Similarly, this Article does not address arguments that government insiders who reveal national security information are

---

10. 446 F.2d 1322, 1326 (D.C. Cir. 1971) (Wright, J., dissenting). The quotation is worth setting out in full:

> With the sweep of a rubber stamp labelled "top secret," the executive department seeks to abridge the freedom of the press. It has offered no more. We are asked to turn our backs on the First Amendment simply because certain officials have labelled material as unfit for the American people and the people of the world. Surely, we must demand more. To allow a government to suppress free speech simply through a system of bureaucratic classification would sell our heritage, far, far too cheaply.

Id.

11. *See, e.g.*, Mary-Rose Papandrea, *Lapdogs, Watchdogs, and Scapegoats: The Press and National Security Information*, 83 IND. L.J. 233, 248-49 (2008); Papandrea, *supra* note 1.

engaging in "conduct" and not "speech" (as the government has argued in litigation); that government employees have waived their First Amendment rights by signing contracts agreeing not to reveal classified information; or that government insiders have no First Amendment right to reveal information they obtained during the course of their employment. All of these arguments are important to address, but because I have addressed them elsewhere,[12] I will not repeat my analysis here.

Some readers may question the value of this project given that the law may very well play a small role in decisions about what information is kept secret and what information is disclosed and published. Although traditional journalists frequently claim that their publication decisions are based on a determination of the information's public value, as well as the potential harm that the disclosure of the information might cause, the law does not expressly acknowledge the value of the information to the public.[13] The government likewise has never prosecuted a news organization for disclosing national security information.[14] The decision not to prosecute may have little to do with the applicable standard the government would have to satisfy and more to do with an evaluation of other issues, like concerns about graymail[15] and public resistance to prosecutions.

Nevertheless, we must keep in mind the culture of secrecy and loyalty that is pervasive in the national security infrastructure in this country. Leakers face not only the risk that the First Amendment will not in fact protect their disclosures, even under the approach this Article suggests, but also a whole host of personal and professional incentives not to leak. Furthermore, recent revelations regarding the government's surveillance of national security

12. *See* Papandrea, *supra* note 1, at 514-17, 520-28.

13. McCraw & Gikow, *supra* note 8 ("[W]hat is 'striking' ... is the absence of any attempt to integrate consideration of the public interest into the applicable legal framework—whether as a defense for a leaker, or as a basis for requiring disclosure of national security information through FOIA, or for determining whether a publisher should be subject to a prior restraint or post-publication penalty.").

14. Stone, *supra* note 8, at 186.

15. Azar v. Ashcroft 585 F.3d 559, 578-79 (2d Cir. 2009) ("'[G]raymail ... [is] individual lawsuits brought to induce the [government] to settle a case (or prevent its filing) out of fear that any effort to litigate the action would reveal classified information that may undermine ongoing covert operations." (internal quotation marks omitted)).

reporters[16] and prosecutors' willingness to use subpoenas to compel reporters (like James Risen) to reveal their sources[17] indicate that some protection for the underlying leaks is essential. In addition, the dramatic increase in the number of leak prosecutions, the potential for the dissemination of leaked national security information by nontraditional organizations like WikiLeaks, and the growing chilling effect of the government's crackdown on leaks on the free flow of information to the American public, all render the topic of this Article crucially important.[18]

I. THE CURRENT STATE OF THE CRIMINAL LAW

For over a century Congress has struggled to balance the need for an informed public with legitimate national security demands for secrecy. The various statutes criminalizing the unauthorized dissemination and publication of national security information reflect this struggle. Reading the current statutes to determine the applicable culpability standards in the existing statutory framework is not an easy job. It does not help that judicial guidance is in short supply. Despite the recent rise in the number of leak prosecutions, the number of leak prosecutions overall remains rather small.[19] In addition, the government has never prosecuted a traditional news organization.[20] As a result, courts have had rather few opportunities to interpret the relevant statutes. Nevertheless, intent plays a significant role in the current statutory regime, and the legislative history makes clear that this was no accident. Congress believed

16. *Report Finds NSA Surveillance Harming Journalism and Law*, AM. CIV. LIBERTIES UNION (July 28, 2014), https://www.aclu.org/human-rights-national-security/report-finds-nsa-surveillance-harming-journalism-and-law [http://perma.cc/3WZD-Y4S3].

17. Jonathan Mahler, *Reporter's Case Poses Dilemma for Justice Dept.*, N.Y. TIMES (June 27, 2014), http://www.nytimes.com/2014/06/28/us/case-of-james-risen-times-reporter-poses-dilemma-for-justice-department.html?_r=0 [http://perma.cc/Z6HV-XSEE].

18. *Report Finds NSA Surveillance Harming Journalism and Law*, *supra* note 16.

19. Cora Currier, *Charting Obama's Crackdown on National Security Leaks*, PROPUBLICA (July 30, 2013, 3:40 PM), http://www.propublica.org/special/sealing-loose-lips-charting-obamas-crackdown-on-national-security-leaks [http://perma.cc/6X7F-77V9] (stating that prior to the Obama administration only three leaks were prosecuted under the Espionage Act, and although the administration has aggressively pursued national security leakers, it has brought only seven cases under the Espionage Act).

20. *Espionage Act Hearing*, *supra* note 8, at 39-40 (statement of Kenneth L. Wainstein, Partner, O'Melveny & Myers, LLP); Stone, *supra* note 8, at 186.

intent standards could be a meaningful way to distinguish among different types of disclosures based on their blameworthiness.[21]

Prosecutors can—and have—used a wide variety of criminal statutes to prosecute leakers beyond those discussed in detail in this Part, and these statutes use various intent standards. This Article focuses on the statutes that were enacted specifically with the aim of criminalizing the unauthorized disclosure of national security information because these statutes are the ones in which Congress explicitly considered when such disclosures should be punished.

A. Treason

Treason is a specific intent crime. The Supreme Court has explicitly stated that "treason—the one crime deemed grave enough for definition in our Constitution itself—requires not only the duly witnessed overt act of aid and comfort to the enemy but also the mental element of disloyalty or adherence to the enemy."[22] Treason thus has two elements: aid and comfort to the enemy,[23] and adherence to the enemy.

The "aid and comfort" element does not require the government to prove that the attempt to assist the enemy was substantial, complete, effective, or successful.[24] In cases involving the transmission of information, U.S. courts have made clear that it is not necessary for the government to demonstrate that the enemy made use of the information,[25] or as in one case, that the information was even

---

21. *See infra* Part I.A.1.

22. Morissette v. United States, 342 U.S. 246, 265 (1952); *see id.* at 262 n.21 ("[I]nnocence of intention will defeat a charge even of treason." (citing Haupt v. United States, 330 U.S. 631 (1947))); Cramer v. United States, 325 U.S. 1, 62 (1945).

23. "Enemy" is not defined in the Constitution, but the Court has said that the term includes "subjects or citizens of a foreign State at war with our own." The Prize Cases, 67 U.S. (2 Black) 635, 672 (1863). Some scholars have argued that a group like Al Qaeda constitutes the "enemy" because "Al Qaeda has engaged in violent, war-like attacks on the United States." Carlton F.W. Larson, *The Forgotten Constitutional Law of Treason and the Enemy Combatant Problem*, 154 U. PA. L. REV. 863, 920 (2006).

24. *See* Kawakita v. United States, 343 U.S. 717, 738-39 (1952); *Haupt*, 330 U.S. at 644; United States v. Greathouse, 26 F. Cas. 18, 24 (C.C.N.D. Cal. 1863) (No. 15,254) ("It is not essential, to constitute the giving of aid and comfort, that the enterprise commenced should be successful, and actually render assistance.").

25. *See* Chandler v. United States, 171 F.2d 921, 941 (1st Cir. 1948).

received.[26] The Court's treason cases do not expressly require one to act with the enemy's consent or have any sort of direct relationship with the enemy; although in all of the treason cases, the defendants did serve as agents of the enemy.[27] Requiring some sort of direct relationship, agreement, or arrangement with the enemy would seem essential to avoid a dramatic expansion of the Treason Clause.[28] Any number of actions can aid the enemy—from sabotaging a weapons plant to criticizing the United States—but unless the act is done at the behest or at least in cooperation with the enemy, calling the act "treason" seems incorrect.[29]

Although it is not clear that an actor's subjective intent to direct his actions to the enemy plays a role in determining whether he has provided aid and comfort, the Court has held that such intent is essential in determining whether the individual "adhered" to the enemy. For example, in *Haupt v. United States*, the Court affirmed the treason conviction of a German saboteur's father during World War II, but suggested that permitting the jury to consider whether the defendant had benign motives for extending aid to the enemy was appropriate.[30] The trial court in *Haupt* instructed the jury that the intent element was not met if the father provided assistance to his son "as an individual, as distinguished from assisting him in his purpose, if such existed, of aiding the German Reich, or of injuring the United States."[31] The Supreme Court explained that it was up to the jury to weigh the evidence regarding the father's motivations for assisting his son, which included the defendant's argument that he was just trying to assist his offspring.[32] The jury in *Haupt* ultimately found the father guilty.[33] The Court affirmed the conviction,

26. *Greathouse*, 26 F. Cas. at 24 (explaining that sending a letter to the enemy that contains intelligence constitutes giving aid and comfort, even if the letter is intercepted before delivery).

27. *See* Tom W. Bell, *Treason, Technology, and the Freedom of Expression*, 37 ARIZ. ST. L.J. 999, 1014-15 (2005).

28. *See id.* at 1031-32 (discussing the effects of this approach on a hypothetical defendant who might be subject to treason prosecution for posting criticism of U.S. military policy).

29. *See id.* at 1033 ("Taken at face value, the law reaches all disloyal public criticism of U.S. military policy made by those who owe allegiance to the U.S.... Yet it is inconceivable that all such expressions would trigger prosecutions for treason.").

30. 330 U.S. 631, 641 (1947).

31. *Id.*

32. *Id.*

33. *Id.* at 644.

reasoning that the jury could have reasonably determined that the father did have intent to betray the United States, given several statements he made indicating his "adherence to the German cause."[34] *Haupt* seems to indicate that juries are entitled to consider a broad range of factors when determining whether a defendant acted with the requisite intent to betray, including circumstantial evidence as well as the act itself, but the jury must ultimately conclude that the defendant acted with a specific intent to betray.

Although treason prosecutions are extremely rare and generally unnecessary in light of other, less stringent statutory provisions that can be used to prosecute the same behavior, the requirement that the government must demonstrate the defendant's specific intent to adhere to the enemy indicates that culpability requirements can play a useful role in determining the moral blameworthiness of those who disclosure national security information without authorization.

For disclosures to WikiLeaks, Corporal Chelsea (Bradley) Manning was prosecuted under Article 104 of the Uniform Code of Military Justice.[35] This law is similar to constitutional treason in many ways, including the availablility of the death penalty as a punishment. Indeed, courts frequently treat military treason as the rough equivalent of civil treason cases, even applying a two-witness rule that the relevant statute does not require.[36] The Military Court of Appeals has held that Article 104 is a general, and not specific, intent crime because it simply requires a defendant to "knowingly" communicate with the enemy.[37] Nevertheless, even this intent requirement can play an important limiting role. In the Manning

34. *Id.* at 641-42.

35. 10 U.S.C. § 904 (2012). This provision defines the crime as follows:

> Any person who—
>
> (1) aids, or attempts to aid, the enemy with arms, ammunition, supplies, money, or other things; or
>
> (2) without proper authority, knowingly harbors or protects or gives intelligence to, or communicates or corresponds with or holds any intercourse with the enemy, either directly or indirectly;
>
> shall suffer death or such other punishment as a court-martial or military commission may direct.

Id.

36. *See* Papandrea, *supra* note 1, at 505.

37. United States v. Batchelor, 22 C.M.R. 144, 158 (C.M.A. 1956) ("Article 104(2) of the Code does not require specific criminal intent of any sort.").

prosecution, the government contended that this requirement was satisfied as long as Manning knew that the communications could reach the enemy, even if that was not Manning's primary intent.[38] Although the trial court rejected the argument that the government had to prove that Manning had specific intent to reach the enemy,[39] the court nevertheless entered a verdict in Manning's favor.[40] The reasons for the court's ruling remain unclear,[41] but it is possible that the court was concerned about the troubling constitutional questions the government's position raised. After all, under the government's approach, an actor is subject to an Article 104(a) prosecution—and the death penalty—whenever he has reason to believe that the enemy reads our publications.

B. The Espionage Act

The Espionage Act, codified as §§ 793-798 in Title 18 of the U.S. Code, comprises some of the most confusing and ambiguous federal criminal law on the books.[42] Despite its title, courts agree that the various provisions of the Espionage Act punish much more than traditional espionage.[43] Not only do some provisions apply to government insiders who disclose national security information to the press, but some also appear to leave open the possibility of

---

38. *See* Papandrea, *supra* note 1, at 506, 507 & n.388.

39. *See id.* at 507 & n.389.

40. *See id.* at 507 & n.393.

41. *Id.* at 507; *see also* Charlie Savage, *Manning Found Not Guilty of Aiding the Enemy*, N.Y. TIMES, July 31, 2013, at Al. Because Manning's lawyers requested specific findings only with respect to the charges for which Manning was found guilty, the judge did not explain the basis for acquitting Manning of the article 104(2) charge in the written findings she issued after announcing her decision. *See* Papandrea, *supra* note 1, at 507 & n.393.

42. *See, e.g.*, Edgar & Schmidt, Jr., *supra* note 2, at 934 ("[T]he legislation is in many respects incomprehensible."); Anthony Lewis, *National Security: Muting the "Vital Criticism,"* 34 UCLA L. REV. 1687, 1698 (1987) ("The espionage sections of the Federal Criminal Code are a singularly impenetrable warren of provisions originally passed by Congress under the stresses of World War I." (footnote omitted)); 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, 222 (2007) (noting that the Espionage Act contains "a number of seemingly overlapping and often ambiguous provisions").

43. *See, e.g.*, United States v. Morison, 844 F.2d 1057, 1063-64 (4th Cir. 1988) (relying on the statute's plain language when holding that 18 U.S.C. § 793(d)-(e) could be applied to charges based on the defendant's disclosure of information to the press).

prosecutions against the press itself, as well as any other downstream publishers (including ordinary citizens).

The United States does not have the equivalent of the United Kingdom's Official Secrets Act that broadly criminalizes all disclosures of classified information.[44] In reality, however, the current statutory framework gives the government vast authority to prosecute both government insiders and outsiders for the unauthorized retention or disclosure of classified information.[45]

Although calls to revise these statutes have persisted for decades, Congress has not reformed them, perhaps because "[t]he effort to clarify would have required firm answers to too many difficult questions."[46] Consequently, prosecutorial discretion and judicial interpretation have filled in the gaps.[47] Courts have struggled to interpret the scienter requirements for many of its provisions. As Harold Edgar and Benno Schmidt remarked in their landmark article examining the legislative history, "the proponents of culpability standards [in the Espionage Act] were more concerned with containing their inclusion than elucidating their meaning,"[48] and as a result, the existing statutes contain "cumbersome and opaque descriptions of mental states."[49]

1. Sections 793 and 794

Sections 793 and 794 are the heart of the Espionage Act of 1917, passed shortly after the United States entered World War I.[50]

---

44. Official Secrets Act, 1989, c. 6 (U.K.), *available at* http://perma.cc./WJA4-B72T.

45. *See* Vladeck, *supra* note 42, at 221-27.

46. 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, 357 (1986).

47. *See id.* at 358 & n.20 (noting that the result of Congress's failure to answer the difficult questions is that the Executive is permitted to "carefully choos[e] attractive targets without any declaration of principle and under vaguely enunciated legal norms"). For example, one court upheld the prosecution of a civil mathematician under § 793(f)(2), which criminalizes the failure of someone entrusted with national defense documents or information "to make prompt report of such loss, theft, abstraction, or destruction [of such material] to his superior officer," even though the defendant was not in the military or government service and did not have a "superior officer." United States v. Dedeyan, 584 F.2d 36, 37 n.1, 40 (4th Cir. 1978) (quoting 18 U.S.C. § 793(f)(2) (1976)).

48. Edgar & Schmidt, Jr., *supra* note 2, at 942.

49. Edgar & Schmidt, Jr., *supra* note 46, at 407.

50. Espionage Act of 1917, Pub. L. No. 65-24, ch. 30, 40 Stat. 217 (codified as amended at

Derived from the Defense of Secrets Act of 1911, much of the legislative history focuses on reactions to President Wilson's desire for legislation that would permit him to censor or punish the publication of national security information and to expand the government's power to punish the gathering and retention of national security information.[51] Concerns about the dissemination of important national security information to the enemy through the newspapers was squarely in the minds of those advocating for these broad powers.[52]

The legislative history indicates that Congress attempted to limit the government's ability to prosecute well-meaning individuals through mens rea standards.[53] Unfortunately, the culpability standard appearing most frequently in these statutes is that the defendant acted with the "intent" or "reason to believe" that the national security information "is to be used" or "could be used" to harm the United States or benefit a foreign nation.[54] It is unclear whether this standard requires the government to prove that the defendant acted with the purpose of harming the United States—a standard that would protect those with benign motives—or whether the "reason to believe" standard permits prosecutions based on recklessness or even negligence.[55]

a. Section 793

The first two provisions of § 793 are aimed at the collecting and copying of national defense information.[56] Congress's primary concern appears to have been the collection of information by agents of foreign governments, but the resulting statute is not, on its face, so limited.[57] Section 793(a) focuses on various categories of physical locations like dockyards, railroads, factories, research laboratories,

18 U.S.C. §§ 793-794 (2012)).

51. Edgar & Schmidt, Jr., *supra* note 2, at 940-41.

52. *Id.* at 941 (noting that sponsors cited the publication of military plans in newspapers during the Civil War).

53. *Id.*

54. 18 U.S.C. §§ 793-794. Between the two sections, "intent" appears four times and "reason to believe" appears six times. *Id.*

55. Edgar & Schmidt, Jr., *supra* note 2, at 942.

56. 18 U.S.C. § 793(a)-(b).

57. Edgar & Schmidt, Jr., *supra* note 2, at 970.

and other places "connected with national defense" and at these locations, criminalizes the collection of "information respecting the national defense with intent or reason to believe that the information is to be used to the injury of the United States, or to the advantage of any foreign nation."[58] Section 793(b) criminalizes the copying, taking, making, or obtaining of various documents, like blueprints, photographic negatives, and maps "of anything connected with the national defense" when it is done "for the purpose aforesaid, and with like intent or reason to believe."[59]

Despite objections that "information respecting the national defense" is a potentially limitless category, including "every part ... of the national economy and everything tending to disclose the national mind,"[60] Congress rejected attempts to limit the scope of the statute to specifically named places or specific categories of information because of concerns that such an approach would not adequately protect sensitive information.[61] Instead, Congress added a scienter requirement, which limited the application of the statute to instances in which the defendant has the "intent or reason to believe that the information is to be used to the injury of the United States, or to the advantage of a foreign nation."[62]

By adding culpability requirements, Congress hoped to protect those who acted with the intent of engaging in public debate on national security issues.[63] Indeed, despite the plain language of the statute, some representatives believed that the law would apply only to those with "a conscious purpose to injure" the United States.[64] As Edgar and Schmidt noted, "The legislative history is replete with declarations that 'evil purpose' is required to violate

58. 18 U.S.C. § 793(a).

59. *Id.* § 793(b) ("Whoever, for the purpose aforesaid, and with like intent or reason to believe, copies, takes, makes, or obtains, or attempts to copy, take, make, or obtain, any sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, document, writing, or note of anything connected with the national defense."). It is not clear why Congress included the language "for the purpose aforesaid" as well as "like intent or reason to believe." The "purpose aforesaid" must be referring to the immediately prior subsection, § 793(a), but that provision does not contain any additional scienter requirements aside from the "intent or reason to believe" standard. *Id.* § 793(a).

60. United States v. Heine, 151 F.2d 813, 815 (2d Cir. 1945).

61. Edgar & Schmidt, Jr., *supra* note 2, at 972.

62. 18 U.S.C. § 793(a)-(b).

63. Edgar & Schmidt, Jr., *supra* note 2, at 991.

64. *Id.* at 995-96.

these laws."[65] The congressional record contains little indication, however, of whether Congress meant by this "intent or reason to believe" requirement that the offender had to intend to harm the United States or benefit a foreign power, or whether it "is to be inferred from action when occurrence of the result is a virtual certainty."[66] Arguably, the culpability standard is mere negligence, or at most recklessness.[67]

It does not appear from the legislative history that Congress intended to cover *all* reckless and negligent behavior.[68] On the one hand, Congress was concerned about the government insider who might sell secrets to make money but claim indifference to how the information will be used.[69] The "reason to believe" standard, if interpreted objectively, successfully achieves this goal. On the other hand, however, this statute appears to cover also just about every act of newsgathering, including those made for or by the press. After all, anyone who collects national security information with the aim of disseminating it to the public has an objective "reason to believe" a foreign enemy could get that information.[70] It does not appear that Congress meant to treat these two categories of potential defendants the same.[71]

Another confusing aspect of these statutory provisions is the requirement that a defendant intend or have reason to believe that the information at issue "is to be used" to the advantage of a foreign country or to harm the United States.[72] This language suggests that an actor must have some awareness of how the information he has obtained will be put to use in order to be held criminally liable. Arguably, this language suggests that the actor must intend or have reason to believe that the *primary* use to which this information will be used is a harmful one, not merely that such an outcome is possible.

---

65. *Id.* at 997.

66. *Id.* at 942.

67. *Id.* at 989-90.

68. *Id.* at 997 ("Entirely absent, despite the 'reason to believe' language, is any indication that Congress understood reckless or negligent behavior to be covered.").

69. *Id.*

70. *Id.* at 998.

71. *Id.*

72. 18 U.S.C. § 793(a) (2012).

Subsections 793(d) and (e) apply most directly to the communication of information to and by the press. Subsection 793(d) provides that anyone in

> lawful[ ] ... possession of ... any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, who willfully communicates, delivers, [or] transmits the same to those not entitled to receive it.[73]

Subsection 793(e) is virtually identical to § 793(d), but it applies to those who have "unauthorized possession" of the listed materials and information;[74] the plain language appears to permit the prosecution of the press or any other government outsider. Both § 793(d) and (e) apply whenever a defendant discloses national security materials or information to "any person not entitled to receive it."[75] The category of recipients is not defined in the statute, but the statute arguably includes members of the news media and applies whenever unauthorized disclosures are made (and even repeated) downstream from the original source.[76] Section 793 authorizes the imposition of fines and/or up to 10 years in prison.[77]

As with § 793(a) and (b), the scienter requirements of § 793(d) and (e) are unclear. Both sections provide that the defendant must have acted with "reason to believe [the information] could be used to the injury of the United States or to the advantage of any foreign nation."[78] Notably, these provisions do not require that a defendant act

---

73. *Id.* § 793(d).

74. *Id.* § 793(e)

75. *Id.* § 793(d)-(e).

76. *See* United States v. Morison, 844 F.2d 1057, 1063 (4th Cir. 1988) (rejecting defendant's argument that § 793 applies only in cases involving traditional espionage and explaining that the statute contains no such limitation and no press exemption); *see also Espionage Act Hearing*, *supra* note 8, at 67 (statement of Stephen I. Vladeck, Professor of Law, American University) ("[T]he text of the Act draws no distinction between the leaker, the recipient of the leak, or the 100th person to redistribute, retransmit, or even retain the national defense information that, by that point, is already in the public domain.").

77. 18 U.S.C. § 793(f).

78. *Id.* § 793(d)-(e).

with the intent to harm the United States or to advantage a foreign nation. Instead, these subsections provide that it is sufficient for a defendant to have reason to believe that the information "could be used" for harmful purposes. In other words, in contrast to the culpability provisions in § 793(a) and (b), which require intent or reason to believe the information "is to be used" for bad purposes, § 793(d) and (e) apparently require the government to demonstrate merely that the actor was aware—or should have been aware—of the possibility that the audience could use the information for nefarious ends.

Whatever this culpability standard means, courts have generally agreed that it modifies only the phrase immediately preceding it: "information relating to the national defense."[79] Some courts have explained that the distinction between tangible and intangible information makes sense because "a defendant will more readily recognize a document relating to the national defense based on its content, markings or design than it would intangible or oral 'information' that may not share such attributes."[80] As a result, in cases involving the communication of the specific tangible items listed in the statute (documents, photographs, etc.), the government does not have to demonstrate that the defendant had any mens rea regarding the harmfulness of those items.[81] This explanation is problematic on a number of levels, not the least of which is that the line between "documents" and "information" is hardly a clear one.[82]

In cases involving the transmission of documents, the only mens rea requirement the government must demonstrate is that the defendant communicated, delivered, or transmitted the items "willfully."[83] The Supreme Court has had several opportunities to interpret "willfully" in other federal statutes and has noted that the word can have "many meanings."[84] At a minimum, the Court has

---

79. *Id.*; *see, e.g.*, United States v. Drake, 818 F. Supp. 2d 909, 917 (D. Md. 2011).

80. *Drake*, 818 F. Supp. 2d at 917.

81. *Id.* (stating that when a defendant is charged with possessing documents, the government need only prove that the defendant acted willfully).

82. *See* Edgar & Schmidt, Jr., *supra* note 2, at 1048-49 (exploring the fuzzy distinction between the two categories). For example, it is unclear whether a government employee's notes summarizing national security information would be a "document" or "information." *Id.*

83. *Drake*, 818 F. Supp. 2d at 917.

84. Bryan v. United States, 524 U.S. 184, 191-92 (1998); *see also* Edgar & Schmidt, Jr., *supra* note 2, at 1038 ("'Willful' is one of the law's chameleons, taking on different meanings

held that the term "differentiates between deliberate and unwitting conduct, but in the criminal law, it also typically refers to a culpable state of mind."[85] Unhelpfully, the Court has said that "willfully" means that a defendant acted with "a bad purpose,"[86] and that "[t]he jury must find that the defendant acted with an evil-meaning mind, that is to say, that he acted with knowledge that his conduct was unlawful."[87] In the same breath, the Court has explained that "bad purpose" simply means that the defendant acted with knowledge that he was breaking the law.[88] Knowledge that one's conduct is unlawful, however, is not the same as having a bad motive. To make matters even more confusing, the Court has interpreted "willfully" more vigorously in cases in which the defendant has "engaged in apparently innocent conduct."[89] Determining what conduct is "apparently innocent" is hardly a straightforward inquiry.

Unfortunately, § 793 and its legislative history contain no clear indication of which meaning of "willfully" Congress intended. Edgar and Schmidt argue that their review of the legislative history indicates that Congress did not intend "willfully" to mean the same thing as the "intent or reason to believe" standard it frequently used, or any other "narrow conception of 'willfully' that looks to motivation."[90] Courts interpreting this mens rea requirement in the context of § 793 have held that the government does not have to demonstrate that the defendant acted with intent to harm the United States or give advantage to a foreign interest.[91]

---

in different contexts.").

85. *Bryan*, 524 U.S. at 191.

86. *Id.* at 191-92 ("As a general matter, when used in the criminal context, a 'willful' act is one undertaken with a 'bad purpose.' In other words, in order to establish a 'willful' violation of a statute, 'the Government must prove that the defendant acted with knowledge that his conduct was unlawful.'" (quoting Ratzlaf v. United States, 510 U.S. 135, 137 (1994))).

87. *Id.* at 193.

88. *Id.*

89. *See id.* at 194-95.

90. *See* Edgar & Schmidt, Jr., *supra* note 2, at 1040, 1042.

91. *See, e.g.*, United States v. Miller, 874 F.2d 1255, 1277-78 (9th Cir. 1989) (holding that the government does not have to demonstrate that the defendant knew he was breaking the law but instead simply that he "voluntarily and intentionally committed the acts charged"); United States v. Morison, 844 F.2d 1057, 1073 (4th Cir. 1988) (holding that "proof of the most laudable motives, or any motive at all, is irrelevant under the statute" (internal quotations omitted)); United States v. Truong Dinh Hung, 629 F.2d 908, 919 (4th Cir. 1980) (upholding verdict when the jury was instructed that a defendant must act "voluntarily and intentionally and with a specific intent to do something the law forbids"); United States v. Drake, 818 F.

Although the plain language of the statute easily includes the information-sharing activities of the press (the press certainly "communicates"),[92] some have argued that the absence of the word "publish" in § 793 indicates that Congress intended to exclude the press.[93] Given the complicated history of the Espionage Act and related statutes, it is doubtful that Congress's word choice is meaningful as a matter of statutory interpretation.[94] The relevant legislative history of these statutes indicates Congress did not intend for these laws to be used against the press, even if the disclosures caused harm to national security interests and the press was well aware of those risks when publishing.[95] The plain language of the relevant statutes, however, does not protect the press or its sources.[96] Courts have not had an opportunity to weigh in on this issue because the government has never brought a prosecution against a news organization for publishing national security information.[97]

Supp. 2d 909, 918 (D. Md. 2011) (rejecting the argument that the "willfully" requirement means the government has to show that the defendant acted with a bad motive); United States v. Kim, 808 F. Supp. 2d 44, 53-54 (D.D.C. 2011) (finding that the government must prove only that defendant knew what he was doing was unlawful).

92. Papandrea, *supra* note 11, at 279 (arguing that in *N.Y. Times Co. v. United States*, 403 U.S. 713 (1971) (per curiam), the concurring opinions of Justices Stewart, White, and Blackmun, combined with the three dissenting Justices, indicate the government would be entitled to a lesser standard if it pursued criminal charges against the newspapers).

93. *See* Vladeck, *supra* note 42, at 124 (making this observation); *see*, *e.g.*, United States v. N.Y. Times Co., 328 F. Supp. 324, 328-30 (S.D.N.Y. 1971), *rev'd*, 444 F.2d 544 (2d Cir. 1971) (en banc), *rev'd*, 403 U.S. 713 (1971) (per curiam).

94. Bellia, *supra* note 8, at 1488-91. In addition, it is not clear whether excluding publications would make any sense, given that the disclosure of information to broad audiences arguably causes more damage. *Id.* at 1491.

95. Edgar & Schmidt, Jr., *supra* note 46, at 393 n.159.

96. Mary-Rose Papandrea, *The Publication of National Security Information in the Digital Age*, 5 J. NAT'L SECURITY L. & POL'Y 119, 124-26 (2011).

97. In *United States v. Rosen*, the government brought charges under § 793 against two members of the American Israel Public Affairs Committee (AIPAC) who had received information from a government employee. The Department of Justice has also allegedly convened a grand jury to prosecute charges against WikiLeak's publisher Julian Assange, who is arguably not distinguishable in any legally relevant way from traditional news organizations. *See* Papandrea, *supra* note 96, at 124-26; *Assange Attorney: Secret Grand Jury Meeting in Virginia on WikiLeaks*, CNN (Dec. 13, 2010, 12:00 PM), http://www.cnn.com/2010/CRIME/12/13/wikileaks.investigation [http://perma.cc/ 6S7S-FE7M]. Whatever reasons the government has for not prosecuting traditional news organizations for violating § 793(e), it is highly unlikely that the absence of the word "publish" in the statute is one of them.

b. Section 794

Section 794 of the Espionage Act, titled "Gathering or delivering defense information to aid foreign governments," is the section of the Act most directly and obviously aimed at traditional espionage activities.[98] Section 794(a) imposes criminal penalties on anyone who "communicates, delivers, or transmits" national security information[99] to any foreign government—friend or foe[100]—or "to any faction or party or military or naval force within a foreign country," provided that the person has the "intent or reason to believe that [the information] is to be used to the injury of the United States or aid a foreign nation."[101] Unlike § 793(d) and (e), the mens rea requirements appears at the outset of the subsection and applies in every case, not just those involving intangible disclosures of information.[102] Finally, the punishments § 794(a) authorizes are much more severe than those in § 793. A defendant convicted under § 794(a) faces up to life in prison or the death penalty in cases involving particularly dangerous categories of information."[103] The penalties this section authorize reveal the more serious nature of the actions prohibited.[104]

As with § 793, § 794(a)'s failure to use the word "publish"— despite its appearance in other provisions of the Espionage Act—might indicate that the subsection does not apply to the press.[105] It is not a stretch, however, to say that the press "communicates" when it publishes.[106] Furthermore, § 794(a) arguably contemplates the use of the press to communicate with foreign powers because it provides that the prohibited communication or transmission of the informa-

98. 18 U.S.C. § 794 (2012).

99. The statute specifically lists the prohibited items: "document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, note, instrument, appliance, or information relating to the national defense." *Id.* § 794(a).

100. Gorin v. United States, 312 U.S. 19, 29-30 (1941) (interpreting the prior statute and concluding that "[n]o distinction is made between friend or enemy").

101. 18 U.S.C. § 794(a).

102. *See id.*

103. *Id.*

104. *See* United States v. Morison, 844 F.2d 1057, 1065 (4th Cir. 1988).

105. *See* Edgar & Schmidt, Jr., *supra* note 2, at 943-44 (arguing that the drafters specifically avoided using the word "publish" in this provision, even though they used that word in § 794(b)).

106. *See supra* notes 92-94 and accompanying text.

tion can be made "either directly or indirectly."[107] As the government argued in its prosecution of Chelsea (Bradley) Manning, someone wishing to communicate with a foreign government could use the press (or other downstream publisher) as an intermediary to communicate the information indirectly to a foreign power.[108]

Section 794(b), which is applicable only "in time of war," covers communications to "the enemy" of specific military information as well as "any ... information relating to the public defense, which might be useful *to the enemy*."[109] Unlike § 794(a), § 794(b) does not require that an offender have "intent or reason to believe" that the disclosed national defense information will be "used to the injury of the United States or to the advantage of a foreign nation."[110] The only relevant intent is the defendant's intent to communicate with the enemy. There is no scienter requirement regarding the harm the disclosure might cause, and there is no requirement that the materials cause national security harm. Instead, the only mention of harm comes in the last catchall phrase indicating that the statute applies to "any other information relating to the public defense, which

---

107. *Id.*

108. Charlie Savage, *Manning Found Not Guilty of Aiding the Enemy*, N.Y. TIMES, July 31, 2013, at A1. *But cf.* Edgar & Schmidt, Jr., *supra* note 2, at 943 (arguing that the "direct or indirect" language is "better read as directed at communication between citizens when the transmitter realizes that his contact is but a link in an intended chain to a foreign recipient").

109. 18 U.S.C. § 794(b) (2012) (emphasis added). The full text of § 794(b) provides as follows:

> Whoever, in time of war, with intent that the same shall be communicated to the enemy, collects, records, publishes, or communicates, or attempts to elicit any information with respect to the movement, numbers, description, condition, or disposition of any of the Armed Forces, ships, aircraft, or war materials of the United States, or with respect to the plans or conduct, or supposed plans or conduct of any naval or military operations, or with respect to any works or measures undertaken for or connected with, or intended for the fortification or defense of any place, or any other information relating to the public defense, which might be useful to the enemy, shall be punished by death or by imprisonment for any term of years or for life.

Id. Note that § 794(b) focuses specifically on communications to "the enemy," rather than § 794(a)'s broader prohibition on communications to any foreign government. The statute does not define enemy or indicate whether there must be a declared war for the statute to apply. *See* Edgar & Schmidt, Jr., *supra* note 2, at 945 (exploring this ambiguity).

110. 18 U.S.C. § 794(a)-(b).

might be useful to the enemy."[111] The penalty provision of § 794(b) carries up to life in prison or the death penalty.[112]

Unlike § 794(a), § 794(b) specifically covers anyone who "publishes" military information,[113] and the use of this word indicates Congress meant for the law to apply to the press.[114] Although there are no cases interpreting this statute, prosecuting most news organizations would be almost impossible in most circumstances given the difficulties of proving purposeful intent to communicate with the enemy, rather than mere awareness that the enemy might read the publication.[115] However, Congress has been aware for over a century that it is possible for a news organization to have the specific intent to aid the enemy.[116] Indeed, the Trading with the Enemy Act of 1917, which was passed contemporaneously with the Espionage Act, required foreign language newspapers to submit translations before publication, demonstrating Congress's concern with treasonous newspapers.[117] Although society often believes that the Internet has given rise to problems never before contemplated, concern about news organizations acting in bad faith is not new.

2. Using Culpability Requirements to Limit the Scope of "Information Relating to National Defense"

Both § 793 and § 794 contain a catch-all provision extending their coverage to "information relating to the national defense."[118] The Espionage Act does not contain a definition of what falls within this category, but on its face, the scope is expansive. The Supreme Court has relied on the culpability requirements in these statutes to restrict the scope of that phrase, and in so doing, reject defense arguments that it is unconstitutionally vague and overbroad.[119] The Court's decision, however, has added another layer of confusion to an already confusing set of statutes.

---

111. *Id.* § 794(b).
112. *Id.*
113. *Id.*
114. Edgar & Schmidt, Jr., *supra* note 2, at 1034-35.
115. *Id.* at 965.
116. *See id.* at 965-66.
117. *Id.*
118. 18 U.S.C. §§ 793-794.
119. *See* Gorin v. United States, 312 U.S. 19 (1941).

In *Gorin v. United States*, the Court held that the term "national defense" contained in a predecessor provision was a "generic concept of broad connotations, referring to the military and naval establishments and the related activities of national preparedness."[120] To prosecute under this clause, the Court held that the government does not have to provide any proof of injury or even potential injury to the United States; it is sufficient that the information could be advantageous to a foreign country.[121] The Court rejected arguments that the language "information relating to national security" was unconstitutionally vague on the ground that the phrase was limited by a scienter requirement that the offender had "reason to believe that the information ... is to be used to the injury of the United States, or to the advantage of any foreign nation."[122]

It is puzzling why the Court thought the mens rea requirement was the best way to place a meaningful limit on an otherwise vague and potentially all-encompassing phrase.[123] Certainly Congress had other options. For example, it could have listed certain categories of information, similar to what it has done in § 798 (communications intelligence information),[124] the Atomic Energy Act of 1954 (nuclear energy and weapons information),[125] or the Intelligence Identities Protection Act of 1982 (information revealing identities of covert agents).[126]

Furthermore, *Gorin*'s explanation of the precise nature of this intent requirement was unclear. The Court stated:

---

120. *Id.* at 27-28. Although this definition of national defense information is potentially limited to military information and tactical plans, lower courts have rejected such a limited construction. *See, e.g.*, United States v. Truong Dinh Hung, 629 F.2d 908, 918 (4th Cir. 1980) (rejecting the defendants' attempt to limit "national defense" information to information concerning military matters); United States v. Boyce, 594 F.2d 1246, 1251-52 (9th Cir. 1979).

121. *Gorin*, 312 U.S. at 29-30 (internal quotation marks omitted).

122. *Id.* at 27-28. This scienter requirement applies only to the disclosure of "information relating to the national defense" and not to any of the other tangible materials listed in the statute. *See* S. REP. NO. 81-2369, at 9 (1950). This premise is clear not only from the plain language of the statute but also from the legislative history. The report from the Senate Judiciary Committee, which added the scienter language to the statute, specifically stated that the phrase "which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation" modified only "information relating to the national defense." *Id.*

123. Edgar & Schmidt, Jr., *supra* note 2, at 1076-77.

124. 18 U.S.C. § 798 (2012).

125. 42 U.S.C. §§ 2011-2297h (2012).

126. 50 U.S.C. § 3121 (2012).

> The obvious delimiting words in the statute are those requiring "intent or reason to believe that the information to be obtained is to be used to the injury of the United States, or to the advantage of any foreign nation." This requires those prosecuted to have acted in bad faith. The sanctions apply only when scienter is established. Where there is no occasion for secrecy, as with reports relating to national defense, published by authority of Congress or the military departments, there can, of course, in all likelihood be no reasonable intent to give an advantage to a foreign government.[127]

It is not clear whether *Gorin* establishes an objective or subjective culpability standard.

In particular, the Court used the phrase "bad faith" in a confusing manner. To some, bad faith suggests a subjective intent to harm the United States or to give an advantage to a foreign power. Indeed, some lower courts have embraced this reading of the same "intent or reason to believe" scienter requirement. For example, in *United States v. Rosen*, Judge Ellis held that the government would have to prove not only that the defendants knew that the national defense information at issue could harm the United States, but also that they had a "bad faith purpose to either harm the United States or to aid a foreign government."[128] In other words, Judge Ellis explained, even if the defendants knew the disclosure of the information could harm the United States or help its enemies, they could not be convicted under the statute if they disclosed the information for "some salutary motive" or "as an act of patriotism."[129] Instead, Judge Ellis held, the disclosure of the information must be *objectively* harmful to the United States, and the defendant must be *subjectively* intending to cause that harm.[130] In fact, the court specifically distinguished between unauthorized communications of national security documents, which did not contain the "intent or

127. *Gorin*, 312 U.S. at 27-28.

128. United States v. Rosen (*Rosen I*), 445 F. Supp. 2d 602, 626 (E.D. Va. 2006); *see also* United States v. Troung Dinh Hung, 629 F.2d 908, 919 (4th Cir. 1980) (approving a jury instruction that "defined bad faith as a 'design to mislead or deceive another ... [meaning] not prompted by an honest mistake as to one's duties, but prompted by some personal or underhanded motive'").

129. *Rosen I*, 445 F. Supp. 2d at 626.

130. *Id.* at 640-41, 641 nn.55-56.

reason to know" limitation, and the unauthorized communication of national security information, which did contain that limitation.[131] The government could prosecute the former, Judge Ellis explained, even if the defendants acted with "some salutary motive."[132]

Some courts have expressed doubts about Judge Ellis's reading of the "intent or reason to believe" language.[133] The most fundamental objection is that a "bad faith" requirement does not appear in the plain language of the statute. As one district court held, "the text of the statute means what it says ... 'the possessor ha[d] reason to believe [that the information] could be used to the injury of the United States or to the advantage of any foreign nation.'"[134] Furthermore, some courts have questioned whether an additional mens rea requirement is necessary in cases involving past or present intelligence officers who "had a recognized obligation not to divulge classified, national defense information to those not entitled to receive it."[135] In such cases, the courts have explained, an additional mens rea requirement should not be necessary to satisfy the due

131. *Id.*

132. *Id.* at 625; *see also* United States v. Rosen (*Rosen II*), 520 F. Supp. 2d 786, 793 (E.D. Va. 2007) ("These are glosses on the statutory willfulness requirement that also require the government to prove, in cases involving oral disclosures rather than document disclosures, that the defendant had a bad faith purpose to harm the United States or to aid a foreign government."); United States v. Smith, 592 F. Supp. 2d 424, 429 (E.D. Va. 1984) (citing *Gorin*'s "bad faith" language and concluding that "the government must prove beyond a reasonable doubt that the accused had the requisite intent to injure this country or aid a foreign government").

133. *See*, *e.g.*, United States v. Rosen (*Rosen III*), 557 F.3d 192, 199 n.8 (4th Cir. 2009) (stating in dicta that although it lacked jurisdiction to review Judge Ellis's interpretation of that clause, "[w]e are nevertheless concerned by the potential that the [district court order] imposes an additional burden on the prosecution not mandated by the governing statute"); United States v. Miller, 874 F. 2d 1255, 1277-78 (9th Cir. 1989) (holding "bad faith" language in *Gorin* simply requires the prosecution to prove that the defendant "voluntarily and intentionally committed the acts charged"); *Truong Dinh Hung*, 629 F.2d at 918 (rejecting defendants' arguments that § 793(e) required the government to demonstrate that they acted with "evil intent, *i.e.*, intent to injure the United States or to aid a foreign nation"); United States v. Kiriakou, 898 F. Supp. 2d 921, 924-27 (E.D. Va. 2012). In the few cases involving prosecutions under the information clause of § 793(d), the government has not been required to prove that the disclosures were made in bad faith. *See, e.g.*, *Kiriakou*, 898 F. Supp. 2d at 925-26 (citing United States v. Abu-Jihaad, 630 F.3d 102, 135 (2d Cir. 2010); United States v. Kim, 808 F. Supp. 2d 44, 55 (D.D.C. 2011)); *see also id.* at 926 (discussing military court decisions rejecting arguments that the government must demonstrate that the defendant acted out of bad motive).

134. *Kiriakou*, 898 F. Supp. 2d at 926 (quoting 18 U.S.C. § 793(d)).

135. *Id.* at 925 (internal quotation marks omitted).

process concerns[136] that were arguably present in *Rosen*, which involved the prosecution of two government outsiders. This support draws support from legislative history, which indicates that the drafters did not believe an additional mens rea requirement was necessary because it applied to "persons presumably in closer relationship to the Government which they seek to betray."[137]

Another potential reading of *Gorin* is that the primary purpose of the scienter requirement is to make sure that innocent acts are not punished. In other words, even if the act objectively causes harm to national security, it is essential to determine whether the defendant himself knew of that potential harm.[138] As one court concluded when faced with a similar intent provision in a federal sabotage statute, the only intent required is the intent to interfere with a facility essential for national preparedness.[139] The defendant's patriotism, religious motivation, or other benign purpose for committing those acts is irrelevant.[140]

A close reading of *Gorin* suggests that the Court did not mean to embrace a subjective standard. After stating that a defendant has to act "in bad faith," the Court went on to discuss how "information relating to the national defense" has "a well understood connotation."[141] The Court concluded that the information the defendants communicated was the sort of information that would be objectively useful for a foreign country.[142] The Court also favorably cited one of its prior decisions holding that the jury decides "[w]hat interpretation ought to be placed upon the pamphlet, what would be the

136. *Id.* at 924.

137. *Id.* at 925 (quoting United States v. Morison, 844 F.2d 1057, 1073 n.26 (4th Cir. 1998)).

138. *Cf.* United States v. Kabat, 797 F.2d 580, 587 (8th Cir. 1986) (relying on *Gorin* to interpret similar language in the Sabotage Act, 18 U.S.C. § 2155). The court in *Kabat* stated, "The scienter requirement of section 2155 protects those who do not recognize the military uses of property against which they do violence." *Id.* Another case interpreted the Sabotage Act and explained that "[t]he inclusion of a scienter requirement decreases the likelihood that a person of common intelligence would not understand what conduct the statute prohibits and reduces the chance that the statute will reach innocent conduct." United States v. Walli, No. 3:12-CR-107, 2013 WL 1773617, at *5 (E.D. Tenn. Mar. 11, 2013).

139. *Kabat*, 797 F.2d at 587.

140. *Id.*

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

142. *Id.* at 29 (explaining various ways in which a foreign entity might use the information the defendants provided).

probable effect of distributing it in the mode adopted, and what were defendants' motives in doing this."[143] In that previous decision, however, the Court held the defendants' knowledge of the contents of the pamphlet "of itself furnished a ground for attributing to them an intent to bring about, and for finding that they attempted to bring about, any and all such consequences as reasonably might be anticipated from its distribution."[144] Indeed, Justices Holmes and Brandeis dissented in that case, arguing that, among other things, there was not "a particle of evidence that these statements were made with intent to interfere with the operation or success of the military and naval forces," and that "[s]o far as there is any evidence bearing on the matter of intent, it is directly to the contrary."[145] They pointed out that the only evidence of intent was the leaflet itself.[146] Given that *Gorin* was decided in 1941, when the Court's First Amendment jurisprudence was still in infancy, it is not surprising that the majority of Justices appeared to embrace a standard consistent with the Court's Espionage Act decisions from the same time period.

Another puzzling aspect of *Gorin* is its assertion that "[w]here there is no occasion for secrecy, as with reports relating to national defense, published by authority of Congress or the military departments, there can, of course, in all likelihood be no reasonable intent to give an advantage to a foreign government."[147] It is unclear whether publicly available information can ever constitute national defense information covered under the Espionage Act, or whether the fact that information is publicly available is simply a factor to be taken into account when determining if the defendant had the requisite intent to aid a foreign government. The fairest reading of the quoted language from *Gorin* is the latter, but it is hardly clear this makes any sense. If the disclosure of the information at issue does not pose any risk of injury to the United States or give an advantage to a foreign nation, the defendant's intent does not seem relevant. In addition, the defendant's intent does not seem obviously

143. *Id.* at 32 (quoting Pierce v. United States, 252 U.S. 239, 250 (1920)).

144. *Pierce*, 252 U.S. at 249.

145. *Id.* at 271 (Brandeis, J., dissenting).

146. *Id.* at 272 ("No evidence of intent ... was introduced unless it be found in the leaflet itself.").

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

connected to the secrecy, or lack thereof, of the national security information.[148]

Whether the required intent is the subjective intent to harm the United States or constructive harm based on the reasonable consequences of their speech, what harm is sufficient to constitute "injury to the United States" remains unclear.[149] 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. The Court has sometimes accepted the legitimacy of this argument, particularly in the context of government insiders.[150] And to a certain extent, the extensive document dumps by leakers like Chelsea (Bradley) Manning might harm our national security interests because they can have a chilling effect on the free flow of information and communications among U.S. government officials who "can no longer assume that their off-record, secretive communications among themselves can remain confidential."[151] Another problem with proving harm is that it is impossible to know whether our friends or enemies already have access to the revealed information.[152]

But it may not even matter whether the disclosed information could harm the United States, as long as it might advantage a foreign power. The statute does not define "advantage." Any piece of information relating to the national defense could help its recipient in some way. As a result, the alternative grounds for criminal liability—that the information "harms" the United States—is arguably "surplusage because it is improbable for the United States to be injured except by conduct which also advantages some foreign nation."[153]

---

148. *See* Edgar & Schmidt, Jr., *supra* note 2, at 980.

149. *See* United States v. Hitselberger, 991 F. Supp. 2d 101, 105 (D.D.C. 2013) (holding that defendant had no standing to make this argument because he was charged under only the "document clause" of § 793(e), which does not contain the additional mens rea requirement).

150. *See, e.g.*, Snepp v. United States, 444 U.S. 507, 510-11 (1980).

151. Mark Fenster, *Disclosure's Effects: WikiLeaks and Transparency*, 97 IOWA L. REV. 753, 777 (2012).

152. *See* Posner, *supra* note 8, at n.2 ("It turns out to be exceptionally difficult to prove that disclosures cause harm because one can rarely rule out the possibility that the enemy already has the information.").

153. Edgar & Schmidt, Jr., *supra* note 2, at 988.

It is important to keep in mind that when *Gorin* was decided in 1941, the classification system for sensitive information did not exist. Later courts have noted that classification of information is probative, although not conclusive, evidence that the information relates to the national defense.[154] To be constitutional, lower courts have first required that the information at issue not be publicly available,[155] and the information, if disclosed, must be "potentially damaging to the United States or might be useful to an enemy of the United States."[156] Furthermore, lower courts have narrowly interpreted the *Gorin* exception for national security information that is not secret. For example, the Fourth Circuit has held that the fact that some of the information at issue is publicly available is irrelevant if that information was not made publicly available by the government in an official document.[157]

C. Other Relevant Statutes

Issues of intent have arisen in debates surrounding other laws aimed at punishing the unauthorized disclosure of national security information.

1. Specific Categories of Information

In the decades following the Espionage Act, Congress passed additional legislation targeting the unauthorized disclosures of specific

154. United States v. Morison, 844 F.2d 1057, 1071 (4th Cir. 1988) (rejecting defendant's challenge to "potentially damaging" jury charge based on circuit precedent); *Rosen I*, 445 F. Supp. 2d 602, 623-24 (E.D. Va. 2006).

155. *See, e.g.*, Gorin v. United States, 312 U.S. 19, 28 (1941) (explaining that if the information is not in fact secret, "there can, of course, in all likelihood be no reasonable intent to give an advantage to a foreign government"); United States v. Heine, 151 F.2d 813, 816 (2d Cir. 1945) (holding that compiling and disseminating publicly available information to Germany concerning the production of airplanes in the United States did not constitute a violation of the Espionage Act because none of the transmitted information was secret).

156. *Morison*, 844 F.2d at 1071; *see also Rosen I*, 445 F. Supp. 2d at 621-22.

157. *See*, *e.g.*, United States v. Squillacote, 221 F.3d 542, 577-80 (4th Cir. 2000); *see also* United States v. Marchetti, 466 F.2d 1309, 1318 (4th Cir. 1972) ("Rumor and speculation are not the equivalent of prior disclosure, however, and the presence of that kind of surmise should be no reason for avoidance of restraints upon confirmation from one in a position to know officially.").

categories of national security information with limited intent standards—in some cases, virtually none at all.

For example, § 798 specifically criminalizes "knowingly and willfully" communicating, transmitting, furnishing, or publishing "classified information ... concerning the communication intelligence activities of the United States."[158] Although this statute is broadly applicable to government insiders and outsiders alike, the statute does not require an offender to have "intent or reason to believe" that the publication would harm the United States or provide an advantage to a foreign power. The legislative history demonstrates that the government does not have to prove that the defendant acted with a motive to harm the United States or aid a foreign entity.[159]

Another example is the Atomic Energy Act of 1954, which protects the secrecy of information relating to nuclear energy and weapons.[160] The Act subjects anyone who "communicates, transmits, or discloses" documents or information "involving or incorporating Restricted Data" with the "intent to injure the United States" or advantage a foreign nation,[161] or who has "reason to believe such data" would have that effect to criminal penalties.[162] Those who act with "intent" to advantage a foreign nation or harm the United States face possible life imprisonment and a $100,000 fine, whereas those who act with mere "reason to believe" that the information could advantage a foreign nation face a maximum of ten years in jail and a $50,000 fine.[163] These provisions apply regardless of whether the offender obtained the documents or information at issue "lawfully or unlawfully."[164] Those who receive, attempt to receive, or conspire to receive documents or information "involving or incorporating Restricted Data" can also be prosecuted under another provision provided they act "with intent to injure the United States or with intent to secure an advantage to any foreign nation."[165]

158. 18 U.S.C. § 798 (2012).
159. *See* Edgar & Schmidt, Jr., *supra* note 2, at 1065.
160. *See, e.g.*, 42 U.S.C. § 2274(a) (2012).
161. *Id.* § 2274.
162. *Id.* § 2274(b).
163. *Id.* § 2274(a)-(b).
164. *Id.* § 2274.
165. *Id.* § 2275.

In addition, government employees, contractors, and military officials can be punished for "knowingly" communicating "Restricted Data" to any person not authorized to receive it as long as the offender did so "knowing or having reason to believe that such data is Restricted Data."[166] In such a case, it is not necessary that a person communicate Restricted Data with the intent to harm the United States or advantage a foreign nation, or with reason to believe the communication would have such effect. The Act also specifically authorizes the government to obtain injunctive relief to prevent any violations of its provisions.[167] In *United States v. Progressive, Inc.*, a federal district court relied on the Atomic Energy Act to grant a preliminary injunction to prevent the publication of a magazine article describing a method of manufacturing and assembling a hydrogen bomb.[168]

A third example of legislation aimed at a specific category of national security information is the Intelligence Identities Protection Act of 1982 (IIPA), which prohibits the identification of covert agents.[169] The debate surrounding the enactment of this legislation focused extensively on the appropriate culpability standards as a possible means for protecting well-meaning publications. Under the first two provisions of the IIPA, which are directed at past or present government employees, contractors, or military officials, anyone with authorized access to classified information that identifies a covert agent is prohibited from "intentionally disclosing" that information to any individual not entitled to receive it.[170] The statute does not require the defendant to have any particular motive for the disclosure.[171]

---

166. *Id.* § 2277.

167. *Id.* § 2280.

168. 467 F. Supp. 990, 996 (W.D. Wis. 1979). Unlike the Espionage Act, the Atomic Energy Act specifically authorizes the Attorney General to seek injunctive relief against someone who "has engaged or is about to engage" in any violation of its provisions. 42 U.S.C. § 2280. In *Progressive, Inc.*, the district court held that it would have granted prior restraint even in the absence of an authorizing statute because of the likelihood of "grave, direct, immediate and irreparable harm to the United States." *Progressive*, 467 F. Supp. at 996.

169. 50 U.S.C. § 3121 (2012).

170. *Id.* § 3121(a)-(b).

171. *Id.* The only qualifications on criminal liability are that the discloser of information has knowledge that the information identifies the agent and that the United States is taking affirmative steps to conceal the identity of that agent. *Id.*

The third provision of the IIPA prohibits anyone outside the government from disclosing information identifying a covert agent to anyone not entitled to receive classified information.[172] This portion of the statute is not limited to the disclosure of classified information. As the committee report explained, a person could be prosecuted under this statute for publishing information obtained through a "comprehensive counterintelligence effort of engaging in physical surveillance, electronic surveillance abroad, and other techniques of espionage directed at covert agents."[173]

The legislative history reflects concern about criminalizing constitutionally protected speech, such as academic studies or reports in the media of intelligence failures.[174] Earlier proposed versions required the government to prove that the disclosure of the identity of a covert agent was made "with the intent to impair or impede foreign intelligence activities."[175] Some critics complained that this sort of subjective intent standard would not protect journalists because the fact-finder might accept a history of reporting critical of the United States as evidence of a bad intent.[176] At the same time, the government was concerned that an intent standard could make it unduly difficult to prove beyond a reasonable doubt that a defendant intended to impede foreign intelligence activities and could lead to graymail.[177]

---

172. *Id.* § 3121(c) ("Whoever, in the course of a pattern of activities intended to identify and expose covert agents and with reason to believe that such activities would impair or impede the foreign intelligence activities of the United States, discloses any information that identifies an individual as a covert agent to any individual not authorized to receive classified information ... shall be fined ... or imprisoned.").

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

174. *Id.* at 41-55.

175. *Proposals to Criminalize the Unauthorized Disclosure of the Identities of Undercover United States Intelligence Officers and Agents: Hearing on H.R. 5615 Before the Subcomm. on Legis. of the H. Permanent Select Comm. on Intelligence*, 96th Cong. 156, 158 (1980); *see* H.R. REP. NO. 96-1219, pt. 1, at 2, 6-7 (1980).

176. *Intelligence Identities Protection Legislation: Hearings on S. 2216 Before the S. Select Comm. on Intelligence*, 96th Cong. 22 (1980) [hereinafter *S. 2216 Intelligence Hearings*] (testimony of Robert L. Keuch, Associate Deputy Att'y Gen. of the United States); *cf. id.* at 154-155 (written statement of Ford Rowan, Att'y, Former NBC Correspondent) (noting that sometimes the media *wants* to "impair and impede" an intelligence activity that undermines the moral stature of the United States).

177. *See* Berman & Halperin, *supra* note 173, at 43. Prosecutors who are "graymailed" may instead choose not to pursue a case. Floyd Abrams, a prominent First Amendment lawyer,

Congress abandoned the bad intent standard in favor of a more objective "reason to believe standard" and coupled it with a requirement that the exposure be part of a "pattern of activities intended to identify and expose covert agents."[178] By changing the statute to require a "pattern of activities," Congress attempted to limit the applicability of the statute to those who "make it their business to ferret out and publish the identities of agents," without "affect[ing] the First Amendment rights of those who disclose the identities of agents as an integral part of another enterprise such as news media reporting of intelligence failures or abuses, academic studies of U.S. government policies and programs, or a private organization's enforcement of its internal rules."[179] The committee report also indicated that a reporter would "rarely" have the requisite intent to "identify and expose covert agents," as the law requires.[180] Any proof that a reporter had that intent could be rebutted by evidence demonstrating an alternative, permissible intent, such as the intent to explain questionable government conduct.[181]

2. Espionage-Related Statutes

In addition to the Espionage Act, Congress has passed a number of other laws that target conduct closely related to traditional espionage activities.

Under 18 U.S.C. § 951, it is federal crime to serve "in the United States as an agent of a foreign government without prior notification to the Attorney General."[182] The statute defines "agent of a foreign government" as "an individual who agrees to operate within the United States subject to the direction or control of a foreign

---

conceded that graymail was a possibility, but argued, "I think we are willing as a general matter to live with the proposition that guilty people might even get off because we think we are preserving some other very important rights." *S. 2216 Intelligence Hearings*, *supra* note 176, at 82 (testimony of Floyd Abrams).

178. 50 U.S.C. § 3121(c) (2012).

179. Berman & Halperin, *supra* note 173, at 50-51.

180. *Id.* at 52.

181. *Id.* at 53.

182. 18 U.S.C. § 951(a) (2012). The law excludes diplomatic or consular officers of foreign governments recognized by the Department of State, "any officially and publicly acknowledged and sponsored official or representative of a foreign government," and "any person engaged in a legal commercial transaction." *See id.* § 951(d).

government or official."[183] In *United States v. Dumeisi*, a defendant was convicted of violating this provision based on evidence that he published newspaper articles in an Arabic-language newspaper in the Chicago suburbs pursuant to the directions and instructions of the Iraqi Intelligence Service.[184] The Seventh Circuit held that the conviction did not violate the First Amendment because the district court properly instructed the jury that the defendant could be convicted only if he published these articles pursuant to the direction or control of a foreign government, not simply because he published newspaper articles, which is a constitutionally protected activity.[185]

Federal law also specifically prohibits government employees from communicating classified information "in any manner or by any means, to any other person whom such officer or employee knows or has reason to believe to be an agent or representative of any foreign government."[186] Although the plain language of this statute might support the prosecution of a government insider who gives information to the press in the hopes that it would be disseminated to a foreign government or agent, Edgar and Schmidt conclude that the legislative history indicates the contrary.[187] This statute applies only if the defendant "know[s] or ha[s] reason to know" that the information was classified.[188] Lower courts, however, have held that the government does not have to prove that the information was properly classified.[189] The D.C. Circuit explained that employees can go through the appropriate internal channels to challenge a classification decision, but they cannot challenge the

183. *Id.* § 951(d).

184. 424 F.3d 566, 569-71 (7th Cir. 2005) (affirming conviction). The Fourth Circuit also affirmed a conviction under this provision in *United States v. Truong Dinh Hung*, 629 F.2d 908, 919-20 (4th Cir. 1980).

185. *Dumeisi*, 424 F.3d at 570 (holding jury instructions made clear that defendant's writings, "as well as [his] opinion and political views, are to be considered only insofar as they may pertain to issues of motive and intent").

186. 50 U.S.C. § 783 (2012).

187. Edgar & Schmidt Jr., *supra* note 2, at 1074 ("The legislative history nowhere suggests that such communication would be deemed to have taken place through disclosure of classified information to the press, followed by widespread publication.").

188. 50 U.S.C. § 783(a).

189. *See, e.g.*, Scarbeck v. United States, 317 F.2d 546, 558-60 (D.C. Cir. 1962) ("[W]e think that the inclusion of the requirement for scienter on the part of the employee is a clear indication of the congressional intent to make the superior's classification binding on the employee, once he knows of it.").

classification decision as part of their prosecution.[190] Under a contrary rule, the D.C. Circuit asserted, "[t]he trial of the employee would be converted into a trial of the superior."[191]

D. Lessons from Congress and the Courts

As the foregoing discussion demonstrates, Congress has struggled for over one hundred years to strike the right balance between national security and free speech. The current statutory framework and accompanying legislative history provide valuable lessons regarding the various factors that might be relevant if and when Congress decides to pass revised legislation relating to the collection and dissemination of national security information. The most important lesson is that striking the proper balance between the free flow of information and the need to protect our national security interests is extraordinarily difficult. But beyond that, Congress—as well as courts tasked with interpreting and applying the current laws—has recognized the various different facets of the problem presented.

First, Congress clearly recognizes that traditional espionage poses the greatest danger to our national security. Sections 793(a) and 793(b) are aimed at criminalizing the collection of national security information knowing it would be used to harm the United States or benefit a foreign country.[192] Separate federal laws specifically make it a crime to serve as an agent of a foreign government[193] or to communicate any classified information to any agent of a foreign government, without a showing that the disclosure of the information would cause any sort of harm to the United States or be beneficial to a foreign entity.[194]

Second, the judicial debate about how to interpret *Gorin* reveals concerns about treating government insiders and outsiders in the same way.[195] As some lower courts have recently explained, it might make sense to require prosecutors to demonstrate that government

190. *Id.* at 559-60.
191. *Id.* at 560.
192. *See supra* Part I.B.1.
193. 18 U.S.C. § 951(a) (2012).
194. 50 U.S.C. § 783(a) (2012).
195. *See supra* Part I.B.2.

outsiders are acting with a bad purpose when they disseminate national security information because they are not in a position of trust like government insiders, who are better positioned to know when information concerns national security.[196]

Third, it is apparent that long before the Internet and the WikiLeaks saga Congress was aware that members of the "press"—however that category might be defined—were not entitled to carte blanche immunity from criminal liability for collecting or disseminating national security information. The concern with foreign language newspapers in the early twentieth century reveals this unease.[197] At the same time, Congress primarily directed this concern about the press at the more fringe members of the media establishment, particularly ones that served a foreign audience and, most importantly, did not publish with good motives.

Finally, Congress and the courts share an overwhelming sense of respect for the classification system. Courts have historically been unwilling to second-guess the executive branch's classification system in other contexts—like Freedom of Information Act challenges[198]—so perhaps this should not be terribly surprising. On the other hand, the hesitancy to permit defendants to challenge the propriety of classification decisions is disturbing given the universal consensus that overclassification is rampant and deeply troubling. Congress's deference to the classification system is even more bizarre, given that the classification system is entirely a creature of the executive branch with no input or oversight from Congress. By deferring so completely to the classification system, Congress fails to assert itself as a co-equal branch of government on national security issues.

II. THE FIRST AMENDMENT AND INTENT

In drafting the Espionage Act and related statutes, Congress intended to use scienter requirements to limit the statutes' impact on public discussion of national security issues that are so essential

196. *See supra* Part.I.A.2.

197. *See supra* note 117 and accompanying text.

198. For a sense of this history, see Mary-Rose Papandrea, *Under Attack: The Public's Right to Know and the War on Terror*, 25 B.C. THIRD WORLD L.J. 35, 50-52 (2005).

to a well-functioning democracy. This Part addresses whether this focus on intent has any basis in the First Amendment.

The Supreme Court has indicated in a number of its foundational First Amendment opinions that a speaker's intent—and even at times the speaker's motivation—is relevant in determining the scope of constitutional protection, although exactly what kind of intent matters, why it matters, and when it should matter remains unclear. The Court has focused on different types of intent depending on the type of speech at issue. In some cases, like defamation, privacy, and intentional infliction of emotional distress cases, some statements are protected when speakers do not know that their statements are false or when the speakers are recklessly indifferent to truth or falsity;[199] in other contexts involving the same types of claims, speakers must be at least negligent.[200] The Court has likewise been concerned about an actor's mental state regarding the content of the speech at issue in cases involving obscenity and child pornography.[201] But in other cases involving incitement and freedom of association the Court has suggested that the relevant inquiry is whether the speaker has the specific intent or purpose to achieve a harmful end.[202]

---

199. *See*, *e.g.*, Time, Inc. v. Hill, 385 U.S. 374, 387-88 (1967) (applying an actual malice standard to invasion of privacy claim involving matter of public concern); Garrison v. Louisiana, 379 U.S. 64, 74-75 (1964) (applying an actual malice standard in a criminal libel case involving matter of public concern); N.Y. Times Co. v. Sullivan, 376 U.S. 254, 279-80 (1964) (applying an actual malice test in a civil libel case brought by a public official).

200. Gertz v. Robert Welch, Inc., 418 U.S. 323, 339-40 (1974) (applying a negligence requirement to actual damages and an actual malice test to punitive damages in cases involving private figures and matters of public concern).

201. *See*, *e.g.*, New York v. Ferber, 458 U.S. 747, 764 (1982) (holding that distribution of child pornography is unprotected if the distributor was aware of or recklessly indifferent to the subject's minor status); Smith v. California, 361 U.S. 147, 148-49 (1959) (holding that distribution of obscenity is unprotected if the distributor was aware or reckless about the factual contents of the materials).

202. *See*, *e.g.*, Illinois *ex rel.* Madigan v. Telemarketing Assocs., Inc., 538 U.S. 600, 620 (2003) (upholding fraud standard requiring intent to deceive); Brandenburg v. Ohio, 395 U.S. 444, 447 (1969) (per curiam) (holding advocacy of unlawful acts is unprotected when it is "directed to inciting or producing imminent lawless action and is likely to incite or produce such action"). As mentioned earlier, the U.S. Supreme Court will be deciding whether a defendant must subjectively intend for his communication to be perceived as intimidating in order for his speech to constitute a "true threat," an unprotected category of speech. *See* United States v. Elonis, 730 F.3d 321, 324 (3d Cir. 2013), *cert. granted*, 134 S. Ct. 2819 (2014).

A. The Court's National Security Cases

The Supreme Court has never directly addressed the scope of First Amendment protection for the criminal punishment of unauthorized disclosure or dissemination of national security information, or whether intent should play a role in determining any such protection. This Part briefly summarizes the Court's cases that provide insight on this question.

1. Government Outsiders and Intent

The seminal case on the scope of constitutional protection for disclosures of national security information is *New York Times Co. v. United States* (*Pentagon Papers*), which rejected the government's attempts to obtain an injunction to stop the nation's leading newspapers from publishing a historical study of the Vietnam War.[203] Argued and decided within a matter of days, the case resulted in a brief per curiam opinion that simply stated that the government had not met its "heavy burden" for a prior restraint.[204] Although the Court suggested that the government could obtain an injunction to prevent the dissemination of information that threatened an imminent likelihood of grave harm to national security, the Court did not address the difficult question of what to do when the information posed both a grave risk of harm and high value for public debate.[205] Furthermore, a close reading of the various opinions submitted in the case suggests that a majority of the Justices would permit subsequent criminal punishments under a much lesser standard,[206] although exactly what that standard would be was left unclear.

At least one scholar has argued that the *Pentagon Papers* decision indicated that the Court trusted the newspapers to balance the

---

203. 403 U.S. 713, 714 (1971) (per curiam).

204. *Id.* (holding that the government must bear the "heavy burden of showing justification" when seeking to enforce a prior restraint against the publication of classified national security information).

205. *See* Mary-Rose Papandrea, *Balancing and the Unauthorized Disclosure of National Security Information: A Response to Mark Fenster's* Disclosure Effects: WikiLeaks and Transparency, 97 IOWA L. REV. BULL. 94, 105 (2012), http://ilr.law.uiowa.edu/files/ilr.law.uiowa.edu/files/ILRB_97_Papandrea.pdf [http://perma.cc/EYX4-EJCL].

206. *See* Papandrea, *supra* note 11, at 279-80.

harm and public value of the information in their hands.[207] Because courts have had very few opportunities to consider national security cases involving the traditional media, it is impossible to draw any broad conclusions about the judiciary's willingness to defer to journalistic discretion in the national security context. Nevertheless, just two years after *Pentagon Papers*, the Court expressed concerns with interfering with the press's editorial discretion. In *Miami Herald Publishing Co. v. Tornillo*, the Court explained that "[i]t has yet to be demonstrated how governmental regulation of th[e] crucial process [of editorial control and judgment] can be exercised consistent with First Amendment guarantees of a free press as they have evolved to this time," whether "fair or unfair."[208]

Indeed, in other contexts the Court has generally been very deferential to the publication decisions made by the press and other third parties who publish confidential information. The Supreme Court has decided a long series of cases—often referred to as the *Daily Mail* cases—involving the First Amendment rights of third parties, like the press, to publish lawfully acquired confidential information.[209] These cases do not grant special rights to the press, and the Court has been very careful to refrain from holding that the First Amendment always gives third parties the right to publish truthful information they have lawfully received, noting that the First Amendment would tolerate punishment in cases involving "interest[s] of the highest order."[210] Yet in ruling for third parties in every case it has considered, the Court has relied on a number of general assumptions, including that (1) the government bears the burden of controlling sensitive information, and when it fails to safeguard information, the public generally cannot be held liable for repeating it; and (2) holding third parties liable for repeating sensitive information they have lawfully obtained could have an unwanted chilling effect because they cannot always know what is sensitive and what is not.[211] At the same time, in the most recent

207. *See* Bellia, *supra* note 8, at 1505 ("The *Pentagon Papers* case assured that, once information of high public value was in the hands of the press, the press's assessment would prevail over the government's.").

208. 418 U.S. 241, 258 (1974).

209. *See* Papandrea, *supra* note 11, at 286-96 (summarizing this series of cases).

210. *See*, *e.g.*, Smith v. Daily Mail Publ'g Co., 443 U.S. 97, 103 (1979); Papandrea, *supra* note 11, at 286-87.

211. Papandrea, *supra* note 11, at 294-95.

decision of this series, *Bartnicki v. Vopper*, the Court suggested that balancing value and harm of the information is the appropriate approach.[212] The Court held that the privacy interests in that case "give way when balanced against the interest in publishing matters of public importance."[213]

Although determining this proper balance does not necessarily require an inquiry into the publishers' intent, it does seem to assume a certain level of good faith. None of the individual opinions in the *Pentagon Papers* case discussed the newspapers' intent, but one of the lower court opinions did. In rejecting the government's request for a prior restraint, Judge Gerstein suggested that the good faith intention to inform public debate would protect the *New York Times*:

> I find that there is no reasonable likelihood of the Government successfully proving that the actions of the Times were not in good faith, nor is there irreparable injury to the Government. This has been an effort on the part of the Times to vindicate the right of the public to know. It is not a case involving an intent to communicate vital secrets for the benefit of a foreign government or to the detriment of the United States.[214]

Judge Gerstein's opinion raises the important question of who counts as the "responsible" press, trusted to make difficult editorial decisions about what to publish and what not to publish. Unlike other professions, like attorneys and doctors, journalists are not licensed, and although various journalism associations assert certain journalistic standards, these standards have never been judicially enforceable. One possibility would be to use the Press Clause to give certain publishers special protection to both obtain and publish national security information, but the Court has never relied on the Press Clause in any of its First Amendment decisions, and the difficulties of defining the "press" in any satisfactory way remain daunting, particularly with the rapid changes in the media industry today.[215]

---

212. 532 U.S. 514, 534 (2001).

213. *Id.*

214. United States v. N.Y. Times Co., 328 F. Supp. 324, 330 (S.D.N.Y. 1971), *rev'd*, 444 F.2d 544 (2d Cir. 1971) (en banc), *rev'd*, 403 U.S. 713 (1971) (per curiam).

215. I have explored the difficulties of defining the "press" for purposes of the reporter's

Given the paucity of U.S. Supreme Court cases involving the dissemination of national security information by third parties, it is unclear what the Court would do with such a case. That said, in other contexts, the Court has expressed concern about interfering with the editorial decisions of government outsiders acting with the purpose of informing public debate.[216] In addition, the Court is concerned about establishing rules that would have a chilling effect on the dissemination of information important for public debate.[217] In order to avoid this chilling effect, the Court seems wary of any rule that would impose liability on outsiders who lack, at a minimum, knowledge regarding the sensitivity of the information at issue.[218] *Bartnicki* also offers supports for an approach that balances the costs and benefits of disclosure.[219] Although the Court leaves open the possibility that some information cannot be shared when interests "of the highest order" are involved, the burden remains on the government to demonstrate how any such information would cause clear harm to our national security interests.[220]

2. Government Insiders and Intent

Even though the Court has never directly decided a case involving the unauthorized disclosure of information by a government insider to the press or general public, the cases that the Court has decided do not appear, at least at first glance, to view such disclosures favorably. Upon closer inspection, however, some of the Court's decisions indicate that even in cases involving government insiders, the purpose for the disclosure might make a constitutional difference.

The most damning opinion for government insiders is the Court's heavily criticized decision in *Snepp v. United States*.[221] In this case, the Court imposed a constructive trust on the profits a former CIA employee received from the publication of his book, which he published without going through the contractually required preclearance

privilege in my prior work. *See* Mary-Rose Papandrea, *Citizen Journalism and the Reporter's Privilege*, 91 MINN. L. REV. 515, 564-84 (2008).

216. *See supra* note 208 and accompanying text.

217. *See, e.g.*, Gertz v. Robert Welch, Inc., 418 U.S. 323, 340-41 (1974).

218. *See supra* note 211 and accompanying text.

219. Bartnicki v. Vopper, 532 U.S. 514, 534 (2001).

220. *See supra* note 210 and accompanying text.

221. 444 U.S. 507 (1980) (per curiam).

procedure.[222] In this opinion, the Court declared that the government had a right to a constructive trust even though the book admittedly did not contain any classified information.[223] The Court emphasized that the government had a compelling interest in enforcing the preclearance process in order to protect the "appearance of confidentiality."[224]

Snepp did not address the obvious First Amendment concerns its approach raised, nor did the Court even attempt to reconcile the holding with its prior decision in *Pickering v. Board of Education*.[225] *Pickering* expressly recognized the essential contributions government employees make to public debates, noting that they are the ones "most likely to have informed and definite opinions" on issues relating to their employment.[226] Recognizing that the government "has interests as an employer in regulating the speech of its employee that differ significantly from those it possesses in connection with the regulation of the speech of the citizenry in general,"[227] the Court embraced a balancing test that weighs "the interests of the [employee], as a citizen, in commenting upon matters of public concern and the interest of the State, as an employer, in promoting the efficiency of the public services it performs through its employees."[228]

Although a bright-line rule giving the government absolute authority to restrict the right of its employees and contractors to discuss national security information might pass the *Pickering* balancing test, the *Snepp* decision lacked any such analysis of the interests at stake. Furthermore, this balancing test is unlikely to support such broad authority. It is not clear that the government has a weighty interest in prohibiting insiders from discussing information that is already in the public domain; that does not pose any threat to national security interests; or that reveals the violation of laws, rules, or regulations, gross mismanagement, the waste of funds, abuses of authority, or substantial risks and dangers to public safety.

---

222. *See id.* at 507-08, 510.
223. *Id.*
224. *Id.* at 509 n.3.
225. 391 U.S. 563 (1968).
226. *Id.* at 571-72.
227. *Id.* at 568.
228. *Id.*

It is also worth noting that *Snepp* and *Pickering* alike both arose in the context of civil sanctions against government insiders. Although the Court has made clear that the First Amendment permits the government to exercise greater control over the speech activities in various "managerial domains," including when it is acting as an employer, it is hardly clear that this leeway extends to the imposition of criminal sanctions. Although conceptualizing this difference may be difficult, in the context of government employees and contractors, the importance of this distinction is clear when one considers the power the Court has given the government in public schools. For example, even though schools can punish students with school-related sanctions like suspension and expulsion for speech that substantially disrupts school activities or encourages drug use, the Court has never suggested that the First Amendment would permit the government to prosecute students for this speech.[229]

Pickering did not indicate that an employee's intent was a relevant factor in the balancing test it established, but the potential importance of intent appears in two Supreme Court decisions involving national security information and government insiders. In *Haig v. Agee*, the Court held that the "repeated disclosures of intelligence operations and names of intelligence personnel" were unprotected at least when an ex-CIA agent made these disclosures for "the declared purpose of obstructing all intelligence operations and the recruiting of intelligence personnel."[230] This statement leaves open the possibility that disclosures made for the good faith purpose of informing public debate might be entitled to protection, or at the very least, it might be important to distinguish between those publishers who act in good faith and those who do not. Similarly, in *United States v. Aguilar*, the Court upheld the conviction of a federal judge who revealed the contents of a wiretapping application in violation of a statute that prohibits such disclosures when made "in order to obstruct, impede, or prevent [the wiretapping] interception."[231] The Court specifically noted that in light of the statute's requirements, it was not necessary to engage in any "artificial

229. *See* Papandrea, *supra* note 1, at 534-37 (discussing the constitutional difference between criminal and civil sanctions).

230. 453 U.S. 280, 309-10 (1981).

231. 515 U.S. 593 (1995) (applying 18 U.S.C. § 2232(d)).

narrowing" to accommodate First Amendment concerns.[232] Although *Aguilar* contains some language that is not favorable to the argument that government insiders have a constitutional right to reveal information obtained on the job—especially its comment that some government officials "may have special duties of nondisclosure"[233]—at a minimum the Court's decision is contextually based. *Agee* and *Aguilar* together indicate that the context of a disclosure—including what is disclosed, to whom, and why—might make a constitutional difference even with respect to government insiders.

B. The Role of Intent Generally

In First Amendment law, the speaker's intent frequently plays a major role in determining the availability and scope of constitutional protection,[234] even though a speaker's intent does not usually have any impact on the harm that the speech might cause, or its inherent value.

Intent appears throughout the Court's free speech jurisprudence. In some cases, the relevant intent relates to the speakers' knowledge of the true nature of the content of their speech.[235] Distributors cannot be held strictly liable for selling obscene materials;[236] and distributors of pornography are likewise protected unless they are aware of, or are reckless, regarding the age of individuals depicted in the photographs or videos they sell.[237] Defamation claims against public figures cannot survive without a showing that the speaker acted with actual malice, defined not as ill will or spite toward the subject of his speech but rather as knowledge or reckless indifference regarding the truth or falsity of the challenged statements.[238]

---

232. *Id.* at 606.

233. *Id.*

234. For a more complete survey of intent requirements in the Court's First Amendment cases, see Leslie Kendrick, *Speech, Intent, and the Chilling Effect*, 54 WM. & MARY L. REV. 1633, 1640-48 (2013).

235. Schauer, *supra* note 6, at 220-21 (arguing that the First Amendment's intent standard is not different from intent standards through criminal and civil law that assume that a defendant intends the ordinary and natural meaning of the words he uses).

236. Smith v. California, 361 U.S. 147, 148-49, 155 (1959).

237. New York v. Ferber, 458 U.S. 747, 764-65 (1982).

238. Garrison v. Louisiana, 379 U.S. 69, 74 (1964) (criminal libel case involving public officials); N.Y. Times Co. v. Sullivan, 376 U.S. 254, 280 (1964) (civil libel case involving public official plaintiff).

The same actual malice standard applies to invasion of privacy claims involving matters of public concern.[239] These cases indicate that the First Amendment requires a defendant to have at least some knowledge of the true nature of the speech he is making, but notably they do not require a showing that the defendant intended to cause harm to the plaintiff.

In other instances, however, the Court has held or at least suggested that the defendant's intent to cause harm is a relevant factor in determining the scope of constitutional protection. For example, the Court has held that fraudulent statements are not protected under the First Amendment because they are made with the intent to mislead, not simply because they are false.[240] Similarly, in *United States v. Alvarez*, a plurality of the Court stated that "[w]here false claims are made to effect a fraud or secure moneys or other valuable considerations, say offers of employment, it is well established that the Government may restrict speech without affronting the First Amendment."[241] Both the plurality and Justice Breyer's concurrence expressed concerns that giving the government broad power to restrict intentional lies would have a tremendous chilling effect on free speech.[242] At the same time, in recognizing the constitutionality of perjury statutes and laws forbidding the impersonation of a government officer,[243] the Court made clear that the First Amendment does not *always* require that a speaker intend his false speech to lead to a defined harm. *Alvarez* raises more questions than it answers, but at a minimum, *Alvarez* suggests that a speaker who intends his communications to cause harm is less

239. Time, Inc. v. Hill, 385 U.S. 374, 387-88 (1967) (applying actual malice standard to statutory invasion of privacy claim involving matter of public concern).

240. Illinois *ex rel.* Madigan v. Telemarketing Assocs., Inc., 538 U.S. 600, 621 (2003) (rejecting challenge to fraud action alleging charitable organizations misled potential donors about the amount of their donations that would be used for charitable endeavors because the representations were "made with intent to mislead").

241. 132 S. Ct. 2537, 2547 (2012) (rejecting the government's argument that under Court's precedents, intentional lies fall outside of the First Amendment).

242. *See id.* at 2548 ("The mere potential for the exercise of th[e] power [to penalize any intentional lie] casts a chill, a chill the First Amendment cannot permit if free speech, thought, and discourse are to remain a foundation of our freedom."); *see also id.* at 2553 (Breyer, J., concurring) ("[T]he threat of criminal prosecution for making a false statement can inhibit the speaker from making true statements, thereby 'chilling' a kind of speech that lies at the First Amendment's heart.").

243. *See id.* at 2546 (plurality opinion); *see also id.* at 2554 (Breyer, J., concurring).

likely to be entitled to constitutional protection than those speakers who do not.

Arguably the cases most relevant to the scope of First Amendment protection for the unauthorized dissemination of national security information are the Court's incitement cases. The Court's earliest First Amendment cases involved this topic, and throughout the twentieth century, the Court grappled with the question of when the government could punish speech that incites unlawful conduct. Along the way, the Court incorporated the speaker's intent as a relevant factor in determining the scope of constitutional protection.

In its initial cases, the Court held that the speaker's intent to bring about an unlawful end, combined with the "tendency" of the speech to do just that, satisfied the requirements of the First Amendment even if the unlawful conduct never came to pass. Justice Holmes, writing for the majority in *Schenck v. United States*, suggested that as long as a defendant had the intent to bring about an unlawful act, and the speech had a "tendency" to achieve that end, success is not required.[244] What exactly this requisite "intent" was, however, was unclear. In *Abrams v. United States*, for example, the Court upheld the conviction of several defendants who had distributed pamphlets criticizing the use of U.S. troops in Russia and America's efforts to interfere with the Russian revolution.[245] The Court concluded that the plain language of the pamphlets revealed the defendant's intent to interfere with the United States' war efforts.[246] In his dissent, Justice Holmes disagreed with the majority's interpretation of the word "intent," explaining that in "ordinary legal discussion" intent simply means "knowledge at the time of the act that the consequences said to be intended would ensue."[247] But to satisfy the First Amendment, Justice Holmes argued, "intent"

244. 249 U.S. 47, 52 (1919) ("If the act, (speaking, or circulating a paper,) its tendency and the intent with which it is done are the same, we perceive no ground for saying that success alone warrants making the act a crime.").

245. 250 U.S. 616, 616-17, 623-24 (1919).

246. *Id.* at 624.

247. *Id.* at 626 (Holmes, J., dissenting). This definition is not quite the same as the constructive intent embraced by the Ninth Circuit in *Shaffer v. United States*, in which the court held that a defendant "must be presumed to have intended the natural and probable consequences of what he knowingly did." 255 F. 886, 889 (1919).

should require evidence that "the "consequence is the aim of the deed," not simply knowledge that the consequence might follow.[248]

Another question was whether intent to incite unlawful conduct would be, by itself, sufficient to support a conviction consistent with the First Amendment. At times, Justice Holmes appeared to embrace this view. In his *Abrams* dissent, Holmes contended that "the present danger of immediate evil *or* an intent to bring it about" would be sufficient to uphold the defendants' conviction.[249] In other words, Justice Holmes would appear to permit criminal liability based on *either* the presence of imminent unlawful acts *or* the intent to inspire listeners to commit criminal acts. If the speech at issue caused imminent unlawful behavior, the intent to incite people to commit those acts was not necessary; on the flip side, intent to incite is sufficient to support a conviction under Holmes's view, even if the speaker was completely unsuccessful.[250]

Under the Court's current standard for incitement, a speaker's intent to cause unlawful conduct is insufficient standing alone to support a conviction. Instead, the Court in *Brandenburg v. Ohio* provided the following test for constitutionally unprotected advocacy of unlawful action: the advocacy must be "directed to inciting or producing imminent lawless action and is likely to incite or produce such action."[251] Arguably, under a plain-language reading of this test, a speaker's subjective intent is not relevant at all. The Court did not use the word "intent"; instead, the Court used the phrase "directed to," which could simply require that a defendant use the explicit or literal words of incitement, and that the only intent that is relevant is that the speaker is assumed to have intended the natural and most reasonable meaning of those words.[252] But most scholars have interpreted *Brandenburg* as requiring that the speaker must have subjectively intended to bring about the imminent

248. *Abrams*, 250 U.S. at 627 (Holmes, J., dissenting).

249. *Id.* at 628 (emphasis added).

250. Kendrick, *supra* note 6, at 1263 ("Holmes posited intent not as a *requirement* but as an *alternative* to the existence of a 'present danger of immediate evil,' which apparently licensed punishment without regard for the speaker's state of mind.").

251. 395 U.S. 444, 447 (1969) (per curiam).

252. Schauer, *supra* note 6, at 218-20.

lawless action,[253] and the Court's subsequent decisions have been consistent with this view.[254]

The Court has been more explicit about the importance of intent in protecting the right of association. In *Scales v. United States*, the Court held that membership in a "subversive" organization could be penalized only if the defendant was an "'active' member," and "not merely 'a ... passive ... or purely technical' member," and that the defendant had not just knowledge of the organization's goals but the "specific intent" to further those illegal ends.[255] The Court explained that this specific intent requirement was important because those individuals who were members of subversive organizations but lack the requisite intent to overthrow the government "may be foolish, deluded, or perhaps merely optimistic," but they were not criminals.[256]

The Court's more recent decision in *Holder v. Humanitarian Law Project* curtailed the reach of the specific intent requirement in *Scales* when the Court rejected a First Amendment challenge to a federal law criminalizing the provision of material support to designated terrorist groups.[257] The Court held that a defendant need not have the "specific intent" to further the goals of a designated foreign terrorist organization, as the plaintiffs had argued in reliance on *Scales*.[258] Instead, the Court held that the First Amendment was satisfied if the defendant knew that the organization was a designated foreign terrorist organization and his actions were "coordinated with or under the direction of" the organization.[259] In

253. Frederick Schauer, *Fear, Risk and the First Amendment: Unraveling the "Chilling Effect,"* 58 B.U. L. REV. 685, 724 (1978) (discussing the intent requirement of the *Brandenburg* test); *e.g.*, Cohen v. California, 403 U.S. 15, 16, 18 (1971) (holding that Cohen's jacket stating "Fuck the Draft" could not constitute incitement because "there [was] no showing of an intent to incite disobedience to or disruption of the draft").

254. *See, e.g.*, Hess v. Indiana, 414 U.S. 105, 106-07, 109 (1973) (per curiam) (holding that that defendant's exclamation that "[w]e'll take the fucking street later," as police attempted to move the crowd of demonstrators off the street so that vehicles could pass, was not incitement because "there was no evidence, or rational inference from the import of the language, that his words were intended to produce, and likely to produce, *imminent* disorder"); *see also Cohen*, 403 U.S. at 18 (appearing to embrace this view in holding that the speech on defendant's jacket was not fighting words).

255. 367 U.S. 203, 205-06, 220 (1961).

256. *Id.* at 229-30.

257. 130 S. Ct. 2705, 2712 (2010).

258. *Id.* at 2718.

259. *Id.* at 2726.

rejecting the plaintiffs' argument that the statute was unconstitutional under *Scales* because it lacked a specific intent requirement, the Court reasoned that "[n]othing about *Scales*" indicated that such an intent was necessary when the defendant had provided material support to designated groups.[260]

The dissent criticized the majority for ignoring the requirements of both *Scales* and *Brandenburg*.[261] Notably, however, the Court was careful to make clear the limits of its holding, explaining that "Congress ha[d] avoided any restriction on independent advocacy" as well as "any [other] activities not directed to, coordinated with, or controlled by terrorist groups."[262] Even though the Court did not discuss the scope of First Amendment protection for activities that might aid terrorist groups but are not aimed at terrorist groups, *Humanitarian Law Project* at least suggests the possibility that a scienter requirement might be necessary to punish such activities.[263]

Because the incitement cases exemplify the Court's struggle to balance free debate against safety and security, it is not surprising that scholars examining the First Amendment right to disclosure of national security information frequently embrace the *Brandenburg* test. But most instances of unauthorized national security information disclosures do not urge others to commit unlawful acts. Instead, it might be best to examine the scope of First Amendment protection for such speech by considering these disclosures as belonging to the broad category of harm- or crime-facilitating speech. Communications falling into this category are those that "make [ ] it easier or safer for listeners or readers ... to commit" bad acts.[264] The constitutional difficulty with this type of speech arises when the harm-facilitating communication has both good and bad purposes, and unfortunately, the Supreme Court has offered no direct guidance on

---

260. *Id.* at 2718.

261. *Id.* at 2733 (Breyer, J., dissenting).

262. *Id.* at 2728 (majority opinion).

263. *Id.* at 2720, 2722.

264. For a lengthy discussion of various types of speech that might fit into this category, *see* Eugene Volokh, Crime-Facilitating Speech, 57 STAN. L. REV. 1095, 1097-1103 (2005). Professor Volokh agrees that "harm-facilitating speech" might be an accurate term to capture the kind of speech with dual purposes, but he settles on "crime-facilitating speech" because most of the speech he discusses involves the facilitation of crimes, and the term "harm" seems "more concrete" because it "could include many harms, including offense, spiritual degradation, and more." *Id.* at 1103 n.45.

how to deal with such communications. The dissemination of national security information arguably falls within this tricky category because it often involves speech that can be used for purposes that are both good (informing public debate) and bad (aiding our enemies or harming the United States).[265]

A mens rea requirement that requires merely *knowledge* that information could be used for bad purposes would subject anyone who shares that information to punishment.[266] Concerns about the ramifications of such a rule are weaker in contexts in which the speaker shares the information with particular persons who are likely to use that information improperly.[267] Instead, the most obvious and potentially most powerful means of distinguishing between speech with good and bad purposes is to examine the context of the communication as well as the intent of the speaker.[268] As with the actual malice inquiry, a fact-finder would not be required to take a defendant's asserted purpose at face value. To judge the veracity of a defendant's good faith defense, the fact-finder could consider the context in which national security information is shared, with a specific focus on the intended audience and the precise nature of the information revealed.

To be clear, the Supreme Court has not been consistent in its invocation of intent standards in defining the scope of free speech rights. In the context of national security information that poses a serious and immediate threat of harm to our national security interests, the Court might very well conclude that good intentions are irrelevant. After all, *Pentagon Papers* arguably suggests that even prior restraints would be permissible in such circumstances,[269] and in *Bartnicki*, the Court was careful to mention that "interests of the highest order" could strip innocent third-party speakers of First Amendment protection.[270] This does not mean that intent is irrelevant in every case, but that in a small subcategory of cases, speaker's intent is not important.

---

265. *Id.* at 1115 (arguing that some disclosures of the government's abuse of its police powers "would indeed be valuable to political discourse when communicated to some listeners, even if it's harmful in the hands of others").

266. *Id.* at 1175.

267. *Id.* at 1176.

268. *Id.* at 1179-81.

269. United States v. Wash. Post Co., 446 F. 2d 1327 (D.C. Cir. 1971).

270. Bartnicki v. Vopper, 532 U.S. 514, 518 (2001).

Furthermore, the Court has not used intent standards consistently. Although this might indicate that we should proceed cautiously before adopting intent standards in yet another context, the Court's inconsistency might be a virtue. Rather than using the same intent standard in every case, perhaps it would be most appropriate to incorporate different intent standards for government insiders and outsiders. For example, it might better reflect the goals of the First Amendment to focus on speakers' mental states regarding the content of the information for government insiders—the sort of inquiry we see in *Sullivan*—but the intent to contribute to public debate for government outsiders, as we see in the incitement cases. The relevant inquiry for government insiders would not be whether they acted with a "bad motive" to help the enemy (or, to put it another way, a "good motive" to contribute to public debate), but rather whether the speaker believed in good faith (even if incorrectly) that the information revealed government wrongdoing. The benefit of focusing on the speaker's mental state regarding the content of the communicated information avoids the problems of giving constitutional protection to all government insiders who spill the nation's secrets claiming they did so with the best of intentions.

III. OBJECTIONS TO IMPOSING AN INTENT STANDARD

As Part I demonstrated, incorporating intent standards into the substantive definition of crimes relating to the dissemination of national security information is not a new idea. Although the current statutory regime is largely incoherent, the text of the relevant statutes as well as the legislative history clearly indicates that Congress has been aware of the usefulness of culpability standards for over a century. Part II demonstrated that even though the Supreme Court's jurisprudence is unclear on when the First Amendment requires some level of culpability, in many instances, the Supreme Court has held that in order to preserve our nation's essential free speech values, the defendant must have knowledge regarding the harmful content of his speech or intent to cause harm with his speech. Nevertheless, the argument that it is important as a matter of criminal law policy and constitutional law to incorporate intent standards when criminalizing the unauthorized disclosure and dissemination of national security information faces myriad

objections. This Section attempts to address the most likely objections.

One of the most frequent objections to requiring a speaker's intent to cause harm is that intent should be irrelevant when the harm is the same; the information will reach not only the American public but our enemies as well.[271] 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.[272] Given the potentially serious consequences of any unauthorized disclosure of national security information, some might argue, mens rea requirements should be as minimal as possible in order to discourage such disclosures and to make it easier to prosecute those that do occur.[273]

As a factual matter, in some instances, there are differences in the harm that spies and leakers cause. Because publishers often keep the identity of their sources anonymous, foreigners may not know whether the information in U.S. news sources is reliable.[274] Another potentially relevant difference between spies and leakers is that in the case of leaks, the United States has the benefit of knowing what secrets are out, and the United States can respond accordingly.[275] In some rare cases, foreign nations or political groups

---

271. *See, e.g.*, *Espionage Act Hearing*, *supra* note 8, at 3 (noting that a motive requirement might be a useful way of distinguishing "the conduct of individuals like Julian Assange from the actions ... of the *New York Times*," but the defendant's motive does not change the harm resulting from the disclosure of national security information); Edgar & Schmidt, Jr., *supra* note 2, at 934 ("[S]ecurity is, by and large, equally compromised by the publication of secrets in newspapers or magazines available to all as it is by their transfer to foreign spies in encoded microdots."); Volokh, *supra* note 264, at 1192 (comparing two reporters who publish records about secret subpoenas of library records and arguing that because the "bad motivation" of one reporter to interfere with the investigation does not decrease the value or increase the harm of his article, "[t]he ability of dual-use crime-facilitating speech to contribute to the exchange of facts and ideas is likewise independent of whether it's motivated by a bad purpose").

272. *See* Edgar & Schmidt, Jr., *supra* note 2, at 1083 ("In our reasonably open society, Congress and the newspapers reveal large amounts of defense information that would be difficult and exceedingly expensive for interested foreign governments to collect on their own.").

273. *See* Jonathan L. Hood, *What is Reasonable Cause to Believe?: The Mens Rea Required for Conviction Under 21 U.S.C. § 841*, 30 PACE L. REV. 1360, 1365-67, 1369-70, 1376 (2010) (arguing that an objective mens rea is generally preferred for crimes with "serious repercussions" to discourage government officials from engaging in harmful behavior, and to ease the prosecutorial burden").

274. Of course the same problem could arise with spies, who might be double agents.

275. That said, changing course might be easier in the case of "easily altered contingency plans" than it would be when a leaker reveals "blueprints for entrenched weapons systems."

might not notice national security information published in a newspaper, a magazine, or online. The most famous example of this occurred in 1942, when the Japanese failed to read a story in the Chicago Tribune revealing that the United States had broken the Japanese code.[276]

But lumping all unauthorized disclosures together ignores a more fundamental problem. Democracies are inherently open societies, and the free flow of information about our government to both citizens and foreigners alike is "a necessary consequence of the nation's deepest values."[277] This does not mean that we give up all hope of preventing the exposure of our most sensitive secrets, but it does mean that the disclosure of some national security secrets is not only inevitable but also essential for the proper functioning of our government. As I have discussed elsewhere at greater length, leaks play a crucial—albeit imperfect—role in checking executive power.[278] Grouping all leaks together, and criminalizing them, would provide the executive branch with undue control over the flow of national security information to the public.

In addition, it is important to recognize that the unauthorized disclosure of national security information can have both harmful and valuable effects.[279] It is truly "dual-use" information. For example, information that reveals gaps in security may alert "bad" people about our vulnerabilities, but this same information may have political value because it reveals that the government is not doing enough to protect us.[280] Allowing these sorts of disclosures may not only stimulate officials to take additional security precautions, but may also provide us with a genuine sense of security based on our confidence that the press would expose any weaknesses.[281] Information about government misconduct that is illegal

---

Edgar & Schmidt, Jr., *supra* note 2, at 934.

276. Editorial, *The Battle of Midway—A Secrets Storm*, CHI. TRIB. (Aug. 11, 2013), http://articles.chicagotribune.com/2013-08-11/opinion/ct-edit-midway-20130811_1_tribune-tower-secrets-u-s-navy [http://perma.cc/SYB9-6DF7].

277. *Id.* at 1083.

278. *See* Papandrea, *supra* note 1, at 464-82.

279. *Id.* at 481; Volokh, *supra* note 264, at 1115 (publishing secret information may be "valuable to political discourse when communicated to some listeners, even if it's harmful in the hands of others").

280. Volokh, *supra* note 264, at 1119.

281. *Id.* at 1120.

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.[282] More detailed disclosures are potentially more useful to our enemies, but they are also more likely to contribute to a meaningful public debate.[283]

Even those who appreciate that all leaks are not alike object that "inquiries into subjective intent and personal motivation are usually fruitless—and often dangerous."[284] Determining whether someone acted for selfish or altruistic reasons is notoriously difficult.[285] 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, such as financial gain, sexual gratification, ideological affinity, or a desire for excitement.[286] This objection is well taken and reveals the tricky distinction between a speaker's intent and motivation. The best response to this objection is to point out that a number of criminal statutes already require the government to prove that defendants have acted with the requisite intent; incorporating intent standards into national security disclosure statutes would not be all that unusual.

Instead of inquiring into a defendant's actual mens rea, one alternative approach is to consider potential proxies for good intentions. One such suggestion is to offer no protection to those individuals who disclose national security information anonymously. Rahul Sagar, along with others, have argued that those who act in good faith to reveal information in service of the public interest should be willing to accept the consequences for their disclosures.[287]

---

282. *Id.* at 1122-23.

283. *Id.* at 1121.

284. Stone, *supra* note 8, at 216.

285. *See, e.g.*, Dirks v. SEC, 463 U.S. 646, 676 n.12 (1983) (Blackmun, J., dissenting) ("The distinction between pure altruism and self-interest has puzzled philosophers for centuries; there is no reason to believe that courts and administrative law judges will have an easier time with it.").

286. *See* Papandrea, *supra* note 1, at 489 (detailing various potential motivations for espionage).

287. RAHUL SAGAR, SECRETS AND LEAKS 134 (2013) ("Requiring a whistleblower to be willing to disclose her identity makes it less likely that even those officials who have good intentions will blow the whistle.").

Sagar's argument echoes a familiar assumption regarding civil disobedience.[288]

But is it really true that willingness to risk personal and professional loss is an accurate proxy for a desire to serve the public interest? Whistleblowers are often ostracized and lose their jobs, families, and friends. The willingness to face the ostracism that often accompanies exposure is more likely a good proxy for foolhardiness than it is for willingness to serve the public interest. Granting protection only to those willing to accept the consequences would have a severe chilling effect on leaks because very few people would be willing to take that risk. Indeed, even Sagar would relax the requirement of exposure in cases involving "gross misconduct" because the public's interest in this information is "overriding."[289]

Although Professor Sagar's approach is flawed, his implicit suggestion that the context of leaks should matter makes sense. Any inquiry into a defendant's subjective intent will not take the defendant's protestations of innocence as the final word on the issue. Instead, it is essential for a fact-finder to consider the nature of the information revealed and to whom it is revealed in evaluating the intent of the speaker.

Another objection is that although an intent requirement may be "logically or morally compelling," it is nevertheless likely to offer defendants very little protection in practice.[290] This concern is particularly apt during wartime or other hostilities, when those who disclose sensitive national security information are frequently labeled unpatriotic traitors.[291] The problem during the early Espionage Act prosecutions was that judges "allow[ed] juries to infer specific intent from the bare possibility that the speaker might have had such an intent."[292] Furthermore, it is easier to present an outsider—like Julian Assange—as having a "bad purpose" to harm the

---

288. *See* Papandrea, *supra* note 1, at 484 n.210 (citing various scholars, including John Rawls, who have argued that true whistleblowers accept that the law will offer them no protection).

289. SAGAR, *supra* note 287, at 137-38.

290. *See* Geoffrey R. Stone, *The Origins of the "Bad Tendency" Test: Free Speech in Wartime*, 2002 SUP. CT. REV. 411, 448 ("[A] standard based primarily on intent, however logical or morally satisfying, fails in practice.").

291. *Id.* ("[I]t is especially dangerous to undertake [an intent] inquiry when jurors, and even some judges, are already inflamed against the defendant because of his 'disloyalty.'").

292. *Id.* at 425.

United States.[293] The Supreme Court has itself recognized the potential futility of intent standards. In *New York Times Co. v. Sullivan*, in which the Court established the actual malice standard, the Court was so concerned that the Alabama courts would reach the exact same decision on remand even with an actual malice requirement that the Supreme Court went out of its way to make clear that the current record would not support a new trial.[294]

The first response to this objection is that it fails to appreciate that intent is not the only relevant element of a crime of unauthorized disclosure. Although in its early incitement cases the Court—including sometimes Justice Holmes—suggested that intent to cause harm, standing alone, would be sufficient to satisfy any First Amendment concerns, the Court has long since moved past that position.[295] This Article is concerned with whether intent places an additional limitation on the government's ability to restrict the disclosures of national security information, not whether some level of intent standing alone would satisfy constitutional concerns.

Intent would be an element that must be proven over and above other elements of the crime. For example, it would be very problematic if Congress were to criminalize the unauthorized disclosure of national security information whenever it happens to be classified, or whenever the information could be "potentially damaging" to the nation's security interests. As one judge has noted, a "potentially damaging" standard has an incredibly broad sweep because "[o]ne may wonder whether any information shown to be related somehow to national defense could fail to have at least some such 'potential.'"[296] Instead, a more appropriate approach might be to allow the government a presumption that classified information is properly classified, but allow a leaker to demonstrate that the information was improperly classified or that the information reveals government wrongdoing.[297]

---

293. Wells, *supra* note 8, at 62.

294. 376 U.S. 254 (1964); Mary-Rose Papandrea, *The Story of* New York Times Co. v. Sullivan, *in* FIRST AMENDMENT STORIES 229, 251 (Richard W. Garnett & Andrew Koppelman eds., 2012).

295. Thomas Healy, Brandenburg *in a Time of Terror*, 84 NOTRE DAME L. REV. 655, 663 (2009).

296. United States v. Morison, 844 F.2d 1057, 1086 (4th Cir. 1988) (Phillips, J., concurring).

297. It would be insufficient to allow defendants to demonstrate only that the information should never have been classified, although that would be an improvement over the current

Another response to concerns that an intent standard would be meaningless is to remind objectors that appellate courts would be required to review the lower court's intent findings, and as in the defamation context, this review could be de novo. Of course, appellate review hardly offers a perfect response to this problem, given that appellate judges can likewise be caught up in the wartime fears and patriotic fever that grip the nation at large. The Court's record since September 11, 2001, however, indicates that the Court is well aware of the mistakes it has made in the past (like *Korematsu v. United States*[298]) and capable of reviewing national security issues with the requisite detachment.[299]

In order to determine the subjective mindset of a discloser, the decision maker will necessarily have to consider various types of objective evidence. As in the context of defamation cases, when the plaintiff bears the burden of demonstrating that the defendant published the challenged statements with actual malice, the defendant's self-serving statements are not taken at their word.[300] Instead, fact-finders routinely examine all the circumstances surrounding the publication decision. In the context of national security information disclosures, the same sort of inquiry would take place. Indeed, in some ways the dichotomy between subjective and objective intentions is false because any analysis of subjective purposes will involve the analysis of objective factors.[301]

Some objections to the incorporation of intent standards are specific to government insiders. Many have argued—and even the Supreme Court has suggested in *Snepp*—that government employees and contractors have waived any First Amendment rights they

---

state of the law, because the current classification system does not forbid the classification of information relating to illegal government activities. *See* Papandrea, *supra* note 1, at 477 (explaining that current executive classification orders prohibit the classification of information that pertains to "violations of law, inefficiency, or administrative error," or classification of embarrassing information, but only when the classification was done with the intent of concealing wrongdoing or embarrassment).

298. 323 U.S. 214 (1944).

299. *See, e.g.*, Hamdi v. Rumsfeld, 542 U.S. 507, 509 (2004) ("[D]ue process demands that a citizen held in the United States as an enemy combatant be given a meaningful opportunity to contest the factual basis for that detention before a neutral decisionmaker.").

300. *See* N.Y. Times Co. v. Sullivan, 376 U.S. 254, 279-80, 283 (1964).

301. *See, e.g.*, Haupt v. United States, 330 U.S. 631, 641 (1947) (holding that a jury could consider evidence to determine whether defendant had requisite intent to adhere to the enemy when he assisted his son, a German saboteur).

might have to reveal national security information they receive on the job, whether explicitly (by signing non-disclosure agreements) or implicitly (by accepting the job and undertaking a position of trust). These arguments prove too much. Government insiders who sign nondisclosure agreements arguably lack bargaining position and full knowledge of the import of their decision to sign such agreements. Although no one is required to take a government job, this argument ignores reality to contend that government insiders have a real "choice" about whether to sign a nondisclosure agreement. In addition, government employees must do so before receiving access to any confidential information. Although it is likely that many government employees are aware of the possibility that they might receive access to information that is in some way disquieting, the fact remains that insiders do not sign these agreements knowing precisely what information they will receive and what sort of moral quandary forced silence will impose on them.

Furthermore, there should be nothing magical about contracts of silence, particularly when the government is one of the signatories. As a matter of contract law, some contracts are plainly unenforceable because they violate public policy. For example, contracts to perform a crime or tortious conduct are generally unenforceable.[302] Contracts to conceal criminal or tortious activity might sometimes be enforceable, but in most situations they are not.[303] I have already addressed the relevant contract and agency law principles at length in another article,[304] and it is sufficient to state here that while the public policy exception to contract law is certainly limited, it does exist and could come into play in a number of leak cases, particularly those that reveal criminal or tortious wrongdoing. The existence of a contract does not eliminate all public policy and First Amendment concerns.

Professor Leslie Kendrick has argued that the strict enforceability of nondisclosure agreements is constitutional because government insiders are punished for "non-message-related harm[s]," rather

302. Alan E. Garfield, *Promises of Silence: Contract Law and Freedom of Speech*, 83 CORNELL L. REV. 261, 295 (1998) (pointing out that "hit-man" contracts are plainly unenforceable); *id.* at 325 (noting that contracts to commit tortious acts are unenforceable).

303. *See id.* at 307-12.

304. *See* Papandrea, *supra* note 1, at 520-33.

than the content of the leaks themselves.[305] The idea is that the government needs to protect against the disclosure of sensitive information because it would inhibit the proper functioning of government not to enforce such contracts strictly. In other words, the government has very good reasons for demanding secrecy from its employees and contractors; its ability to function would be in jeopardy if its confidentiality requirements were not enforceable. This argument is compelling if we were considering a facial attack on all government nondisclosure agreements. But it overstates the case in the context of as-applied challenges.[306] The decision to prosecute one leak rather than the (hundreds of) others is not a content-neutral decision.

CONCLUSION

The public dialogue about the Snowden and Manning leaks, the struggles of Congress and the lower courts to incorporate intent standards in cases involving disclosures of national security information, and the Supreme Court's attention to the role of intent in protecting essential First Amendment rights demonstrate that the intent of the leaker is important as a matter of common sense, public policy, and constitutional law. As Robert Post once noted (albeit in a different context), the argument that intent should not matter is "remarkable" given that "in ordinary life our assessment of the meaning and value of speech often depends upon our understanding of the purposes or intentions of a speaker."[307]

305. Kendrick, *supra* note 6, at 1283.

306. Professor Fred Zacharias makes a similar argument distinguishing facial and as applied attacks in the context of lawyer confidentiality rules. Fred C. Zacharias, *Rethinking Confidentiality II: Is Confidentiality Constitutional?*, 75 IOWA L. REV. 601, 611 (1990) ("Employing facial analysis—like categorizing—makes it far easier to support a rule that only sometimes works.").

307. ROBERT C. POST, CONSTITUTIONAL DOMAINS 152 (1995).