LEAKER TRAITOR WHISTLEBLOWER SPY: NATIONAL SECURITY LEAKS AND THE FIRST AMENDMENT

MARY-ROSE PAPANDREA[*]

[*] Professor, Boston College Law School. Many thanks to David Ardia, Al Brophy, Bernie Burk, John Coyle, Lyrissa Lidsky, Helen Norton, Adam Shinar, Rob Smith, Sonja West, and the participants at Yale Law School's Freedom of Expression Scholars Conference. I am also grateful for a summer research grant from the Patricia and John McHale Fund for Faculty Research as well as the research assistance of Brian Blood, Noah Hampson, Jeff Locke, Eric Lee, Nicholas Maschinot, Alison Tanner, and Jonathan Williams.

INTRODUCTION

The public debate surrounding the Bradley Manning and Edward Snowden leaks involves a "name game": Are they traitors, spies, or whistleblowers? Each of these labels carries "connotations of righteousness and wrongdoing."[1] To the executive branch, however, these labels are irrelevant.[2] It regards all unauthorized disclosures of national security information the same way – regardless of why or to whom the leaks are made – because all leaks expose government secrets and undermine the executive's ability to control the dissemination of information to the public.[3]

Historically the executive branch has seldom pursued criminal leak prosecutions.[4] Consequently, until the recent uptick in leak prosecutions, it was easy to argue that the First Amendment offered no protection to government

[1] Katy Steinmetz, *The Edward Snowden Name Game: Whistle-Blower, Traitor, Leaker*, TIME (July 10, 2013), http://newsfeed.time.com/2013/07/10/the-edward-snowden-name-game-whistle-blower-traitor-leaker, *archived at* http://perma.cc/9S98-EZV3.

[2] *See* JAMES C. GOODALE, FIGHTING FOR THE PRESS: THE INSIDE STORY OF THE PENTAGON PAPERS AND OTHER BATTLES 207 (2013) ("Obama apparently cannot distinguish between communicating information to the enemy and communicating information to the press. The former is espionage, the latter is not."); DANA PRIEST & WILLIAM M. ARKIN, TOP SECRET AMERICA: THE RISE OF THE NEW AMERICAN SECURITY STATE 19 (2011) ("The deep layers of secrecy were to keep terrorists, foreign spies, and reporters away. We [reporters] were in terrible company and often treated accordingly . . . ."); Marisa Taylor & Jonathan Landay, *Obama's Crackdown Views Leaks as Aiding Enemies of the U.S.*, MCCLATCHY (June 20, 2013), http://www.mcclatchydc.com/2013/06/20/194513/obamas-crackdown-views-leaks-as.html#.UkSv9dKsgyo#storylink=cpy, *archived at* http://perma.cc/K7FH-EDND (observing that a Department of Defense document stated "[h]ammer this fact home . . . leaking is tantamount to aiding the enemies of the United States").

[3] *See, e.g.*, Robert S. Litt, Gen. Counsel for the Office of the Dir. of Nat'l Servs., Remarks at the 23rd Annual Review of the Field of National Security Law (Oct. 23, 2013) (transcript archived at http://perma.cc/6P8V-39XQ) ("What the Washington Post reports, al Qaeda knows."). Although the focus of this Article is on the First Amendment rights of government insiders, the press has also been the subject of treason accusations after publishing leaked national security information. I have addressed the First Amendment rights of the press at length in a previous article. *See* Mary-Rose Papandrea, *Lapdogs, Watchdogs, and Scapegoats: The Press and National Security Information*, 83 IND. L.J. 233 (2008).

[4] *See* William E. Lee, *Deep Background: Journalists, Sources, and the Perils of Leaking*, 57 AM. U. L. REV. 1453, 1467 (2008) ("The tacit understanding in Washington is that leaks are seldom subject to criminal action."); Jonathon C. Medow, *The First Amendment and the Secrecy State:* Snepp v. United States, 130 U. PA. L. REV. 775, 832 (1982) ("[P]rosecution is only a possibility, and a remote one at that.").

insiders – including present and former government employees and independent contractors[5] – who reveal national security information without authorization. Indeed, many scholars defending the right of the press to publish secrets simultaneously argue that the First Amendment imposes virtually no limit on the government's ability to punish leakers.[6] This is not surprising, given that arguments that the press has virtual immunity to disseminate national security information are likely to be more palatable if the government has unbridled power to stop the flow of information at its source. It is also easy to make this distinction between government insiders and outsiders when prosecutions against both are more hypothetical than real.

Times have changed. The Obama Administration has undertaken more leak prosecutions than all prior Administrations combined.[7] The wisdom of some of these leak prosecutions, such as the prosecutions of Bradley Manning and

[5] Bd. of Cnty. Comm'rs v. Umbehr, 518 U.S. 668, 668 (1996) (holding that the First Amendment framework for government employees applies to independent contractors).

[6] *See, e.g.*, KENT GREENAWALT, SPEECH, CRIME, AND THE USES OF LANGUAGE 281-82 (1989) (arguing that the government has the power to impose criminal sanctions against government employees who disclose information obtained on the job); Rodney A. Smolla, *Information as Contraband: The First Amendment and Liability for Trafficking in Speech*, 96 NW. U. L. REV. 1099, 1167 (2002) (stating that the First Amendment does not limit the government's ability to stop leaks); Geoffrey R. Stone, *WikiLeaks, the Proposed SHIELD Act, and the First Amendment*, 5 J. NAT'L SEC. L. & POL'Y 105, 111-13 (2011) (claiming that the government can punish employees as long as unauthorized disclosure of classified information is "potentially damaging" to the United States); Eugene Volokh, *Leakers, Recipients, and Conspirators*, VOLOKH CONSPIRACY (May 21, 2013, 12:04 PM), http://www.volokh.com/2013/05/21/leakers-recipients-and-conspirators, *archived at* http://perma.cc/9JX7-LKG5 ("I think it's pretty clear that it's constitutional to outlaw leaks of government information by those who have promised to keep it secret."). *But see* Geoffrey R. Stone, *Free Speech and National Security*, 84 IND. L.J. 939, 961 (2009) (proposing a new standard for disclosures, namely that disclosure of information should only be prohibited when the "potential harm to the national security outweighs the value of the disclosure to public discourse"). A handful of commentators have argued that both leakers and third parties who receive or distribute leaked information are entitled to little or no First Amendment protection. *See, e.g.*, GABRIEL SCHOENFELD, NECESSARY SECRETS: NATIONAL SECURITY, THE MEDIA, AND THE RULE OF LAW 81 (2010) ("In his *Commentaries*, Joseph Story . . . bluntly stated that the idea that the First Amendment 'was intended to secure to every citizen an absolute right to speak, or write, or print, whatever he might please, without any responsibility, public or private . . . is a supposition too wild to be indulged by any rational man.'" (quoting JOSEPH STORY, 2 COMMENTARIES ON THE CONSTITUTION OF THE UNITED STATES 667 (1858))). At least one scholar has argued that leakers and the third parties that publish those leaks should be subject to the same standard. Alan M. Katz, Comment, *Government Information Leaks and the First Amendment*, 64 CALIF. L. REV. 108, 130-32, 141-42 (1976) (arguing that leakers should not be punished until the government can demonstrate reckless disregard for the harm to the government and lack of value for a self-governing public).

[7] Scott Shane & Charlie Savage, *Administration Took Accidental Path to Setting Record for Leak Cases*, N.Y. TIMES, June 20, 2012, at A14.

Thomas Drake, is questionable at best, and demonstrates a disturbing level of prosecutorial overzealousness.[8] The dramatic crackdown on leakers has created a chilling effect on potential sources of national information for the press and, in turn, the public. In addition, the increase in leak prosecutions threatens the work of the press directly. If the government continues to prosecute leaks, it may more frequently issue subpoenas to reporters, as it has done in the Jeffrey Sterling prosecution,[9] or seek information about reporters' communications from third parties, as it did when it obtained the personal and professional phone records for Associated Press reporters without prior notice to them.[10] Most alarmingly, the revelation that an FBI investigator had described in an affidavit a Fox News reporter as "aiding and abetting" the unauthorized disclosure of national security information had led to fears that the government may prosecute members of the press.[11] Commentators have slowly begun to recognize that if leaks play an important role in our society, we should protect not only the media outlets that publish the leaked information, but also the leakers themselves.[12]

Although a few scholars have recognized that penalties against leakers raise legitimate First Amendment issues,[13] most of the scholarship in this area dates

[8] Tricia Bishop, *NSA Espionage Case Closes Quietly; In Plea Deal, Drake Admits "Exceeding Authorized Use" of Computer, a Misdemeanor*, BALT. SUN, June 11, 2011, at A2. (reporting Drake's guilty plea to one misdemeanor count of "exceeding the authorized use of a computer" after originally facing up to thirty-five years in prison on Espionage Act and other charges); Michael Isikoff, *Justice Case Against Alleged Leaker Collapses*, NBC NEWS (June 9, 2011), http://www.nbcnews.com/id/43349086/#.UoQqa2g2lUR, *archived at* http://perma.cc/49RN-G624 (reporting the possibility that the government's case against Drake collapsed because information he disclosed arguably should never have been classified); Fred Kaplan, *A Moderate Verdict*, SLATE (July 30, 2013), http://www.slate.com/articles/news_and_politics/war_stories/2013/07/bradley_manning_wasn_t_guilty_of_treason.html, *archived at* http://perma.cc/NT73-HMN3 (arguing that the decision to charge Manning with the military equivalent of treason, a charge for which he was acquitted, was the result of prosecutorial overzealousness).

[9] United States v. Sterling, 724 F.3d 482, 492, 499 (4th Cir. 2013) (rejecting reporter James Risen's challenge to a subpoena seeking the identity of his source in connection with Jeffrey Sterling prosecution).

[10] Charlie Savage & Leslie Kaufman, *Phone Records of Journalists Seized by U.S.*, N.Y. TIMES, May 13, 2013, at A1.

[11] Michael Calderone & Ryan J. Reilly, *DOJ Targeting of Fox News Reporter James Rosen Risks Criminalizing Journalism*, HUFFINGTON POST (May 21, 2013), http://www.huffingtonpost.com/2013/05/20/doj-fox-news-james-rosen_n_3307422.html, *archived at* http://perma.cc/D72Q-AXAT.

[12] *See, e.g.*, Mika C. Morse, *Honor or Betrayal? The Ethics of Government Lawyer-Whistleblowers*, 23 GEO. J. LEGAL ETHICS 421, 423 (2010).

[13] Vincent Blasi, *The Checking Value in First Amendment Theory*, 1977 AM. B. FOUND. RES. J. 521, 609 ("[P]enalties against 'leakers' should be thought to raise serious First Amendment issues, and not to be available to public authorities as a matter of prerogative."). Heidi Kitrosser recently published an outstanding article arguing, as I do

back to the time of Samuel Morison's prosecution for delivering classified satellite photos to *Jane's Weekly* in 1988.[14] Even more importantly, none of the prior scholarship regarding the rights of leakers has grappled with the complications posed by massive changes in communications technology in the last two decades, including the decline of traditional media as the exclusive arbiter of the flow of national security information between the government and the public. Changes in communications technology and the media have made it exponentially more difficult to make distinctions among the different types of leakers.

This Article focuses on rebutting the prevailing view among the public, commentators, and scholars that leakers lack First Amendment rights. It concludes that these rights are, in fact, substantial. The First Amendment should support the common sense distinction between those who leak information with the purpose and effect of contributing to the public debate, and those who engage in espionage or even treason by giving national security information to foreign countries or organizations.

Part I addresses potential explanations for the recent uptick in leak prosecutions and the important – yet imperfect – role leaks play as part of our government's system of check and balances. Part II summarizes the current statutory and regulatory protections and penalties applicable to traitors, spies, whistleblowers, and other leakers. Part III examines the scope of First Amendment protection for leakers and concludes that, while treason and espionage are not "speech" for constitutional purposes, all other leaks are "speech." Part III also confronts – and dismantles – the prevailing assumption that the First Amendment does not apply to leakers because they received information in a position of trust and because they contractually waived their First Amendment rights.[15]

---

here, that national security leakers enjoy some measure of First Amendment protection, but her article does not focus on the differences between traitors, whistleblowers, and other leakers. Heidi Kitrosser, *Free Speech Aboard the Leaky Ship of State: Calibrating First Amendment Protections for Leakers of Classified Information*, 6 J. NAT'L L. & POL'Y 409, 441 (2013) (arguing for the application of the balancing test in *Pickering v. Board of Education*, 391 U.S. 563 (1968), in the context of civil and administrative sanctions and strict scrutiny for criminal sanctions).

[14] In the 1980s a few commentators argued for a balancing test. *See, e.g.*, James A. Goldston et al., Comment, *A Nation Less Secure: Diminished Public Access to Information*, 21 HARV. C.R.-C.L. L. REV. 409, 457-58 (1986) (advocating for a balancing test that considers the leak's contribution to public discourse).

[15] Other commentators have addressed the enforceability of confidentiality agreements, although not always in the context of national security employees. *See, e.g.*, Alan E. Garfield, *Promises of Silence: Contract Law and Freedom of Speech*, 83 CORNELL L. REV. 261 (1998) (discussing the limits of nondisclosure agreements generally and asking whether there is "something inherently troubling about a promise to suppress one's speech that warrants regulation," *id.* at 264); Lilli Levi, *Dangerous Liaisons: Seduction and Betrayal in Confidential Press-Source Relations*, 43 RUTGERS L. REV. 609, 645-55 & nn.141-52 (1991)

Part IV argues that the First Amendment limits the government's power to bring criminal prosecutions against leakers who are not traitors or spies. Although treason and espionage are not "speech" under the First Amendment, and therefore are not entitled to constitutional protection, these categories must be carefully defined – like every category of unprotected speech – so that they apply only in cases where the defendants intended to communicate with a foreign power (or "enemy," in the case of treason). This Article argues that by carefully considering what was disclosed, why it was disclosed, and to whom it was disclosed, it is possible to discern the leaker's intended audience and make the necessary distinctions among leakers.

This Article also argues that although the First Amendment permits the government, when functioning as an employer, to restrict the speech of government insiders more easily than it can restrict the speech of government outsiders, this power should be limited to the imposition of employment-related civil and administrative sanctions. The Article concludes that the government should be entitled to pursue criminal sanctions against leakers who are neither traitors nor spies only when government outsiders could be prosecuted: that is, when the disclosures pose a direct, grave, and immediate threat to national security that is not outweighed by the public interest in the information.

Under the approach this Article advocates, the government is not powerless to control the unauthorized dissemination of national security information by its employees and contractors. The government retains significantly greater power to pursue employment-related sanctions. This power is not, however, unlimited. The protection the First Amendment provides against such sanctions is quite limited, leaving the government with important means of deterring and punishing leaks.

I. THE CURRENT NATIONAL SECURITY INFORMATION LANDSCAPE

Until recently, the government prosecuted those engaged in traditional espionage activities, but it rarely prosecuted government insiders who disclosed information to the press. Indeed, it is difficult to find any record of leak prosecutions in our country's early history; instead, those who leaked information faced only civil sanctions, like termination from government employment (and perhaps some public disgrace).[16] Before President Obama took office, all prior presidential administrations combined prosecuted a total

(noting that confidentiality contracts are not as absolute as many assume).

[16] SCHOENFELD, *supra* note 6, at 81.

of three leakers.[17] During Obama's presidency alone, however, the Department of Justice has indicted eight.[18]

As I discuss elsewhere,[19] unauthorized leaks provide a wealth of valuable information essential for government oversight and accountability. The nation's deeply flawed classification system makes it hard to know what truly needs to be kept secret, and leaks help combat the executive's tendency to err on the side of secrecy. At the same time, leaks are a highly imperfect and inefficient vehicle through which to challenge excessive secrecy. As technology makes it harder than ever to distinguish among traitors, spies, and whistleblowers, unease about allowing leakers to go unpunished grows.

A. *Possible Explanations for Increase in Leak Prosecutions*

Although Attorney General Eric Holder claims that the sudden increase in leak prosecutions was largely unplanned, President Obama has made clear that stemming the tide of leaks is a high priority for his Administration.[20] The primary causes of the dramatic increase in prosecutions are likely changes in technology and the media, exploding growth of and access to classified information, and a belief that it is especially important in a war against terrorists to protect our secrets vigilantly.

Changes in technology have led government officials to come down hard on leakers in order to stop leaks before they occur.[21] It cannot be a coincidence that the rise of leak prosecutions coincides with the rise of nontraditional media entities like WikiLeaks. For at least the last century, only the nation's leading newspapers and broadcasters published sensitive national security information, and for the most part, these entities have been both cooperative with government officials and responsible in their publication decisions.[22]

---

[17] In the 1970s, Daniel Ellsberg and Anthony Russo were indicted on Espionage Act charges for leaking the Pentagon Papers, but the case against them was dropped due to prosecutorial misconduct. Cora Currier, *Charting Obama's Crackdown on National Security Leaks*, PRO PUBLICA (July 30, 2013, 2:40 PM), http://www.propublica.org/special/sealing-loose-lips-charting-obamas-crackdown-on-national-security-leaks, *archived at* http://perma.cc/L2CZ-CRCW. In the late 1980s, Samuel Morison was successfully prosecuted for disclosing satellite photographs to a British publication; this was the last leaker prosecution until Lawrence Franklin was prosecuted in 2005 for disclosing information about Israel to lobbyists from AIPAC. Kevin Gosztola, *Obama's Aversion to Leaks Channels Reagan*, SALON (June 22, 2013), http://www.salon.com/2013/06/22/obamas_aversion_to_leaks_channels_reagan, *archived at* http://perma.cc/WQ7E-NNWA.

[18] *See* Charlie Savage, *Former F.B.I. Agent to Plead Guilty in Press Leak*, N.Y. TIMES, Sept. 23, 2013, at A1.

[19] Papandrea, *supra* note 3.

[20] Shane & Savage, *supra* note 7.

[21] PRIEST & ARKIN, *supra* note 2, at 276 (stating that the leak prosecutions are intended, "at the very least, to scare government employees with security clearances into not speaking with reporters").

[22] Some might say the mainstream media tends to be more compliant than responsible, at

They have routinely asked the government for guidance on the ramifications of the national security information in their possession and have frequently withheld stories or limited their scope in order to guard against harm to U.S. security interests.[23]

In the digital age, the ability to engage in the mass dissemination of information is no longer reserved to an elite few, and this makes government officials nervous.[24] Those who want to reveal information to the public have a wide variety of foreign and domestic intermediaries to reach their desired audience; indeed, they can forego intermediation entirely and distribute their information directly to the public. From the government's perspective, foreign intermediaries like WikiLeaks are particularly dangerous because they operate outside the conventional Beltway atmosphere in which the media and government's mutually beneficial relationship exists.[25] They also serve very different audiences. The traditional media publishes for a general audience and, and as a result, it is less likely to publish hypertechnical material that is incomprehensible to its readers (but potentially very valuable to the nation's enemies and allies alike).[26] In addition, the government may fear that, given the possibility of leaks from nontraditional sources, even the traditional media will not delay or forego the publication of secrets, given its need to compete in a challenging business environment.[27]

Furthermore, the U.S. media makes its publication decisions in the shadow of federal law, which necessarily affects their publication decisions. Although the standard that the government must meet to prosecute a publisher who discloses national security information is unclear,[28] newspapers like the *New York Times* and *Washington Post* are unlikely to publish national security secrets simply for the sake of publishing secrets.[29] Moreover, the government

least in some instances, because as a repeat player it wants to preserve its good relationship with the government.

[23] *See* Papandrea, *supra* note 3, at 261 ("There may be many reasons why the press is as cooperative as it is with the government.").

[24] Yochai Benkler, *A Free Irresponsible Press: WikiLeaks and the Battle over the Soul of the Networked Fourth Estate*, 46 HARV. C.R.-C.L. L. REV. 311, 313 (2011).

[25] I detail this symbiotic relationship in a previous article. *See* Papandrea, *supra* note 3, at 248-62.

[26] *See* David Pozen, *Leaky Leviathan*, 127 HARV. L. REV. 512, 615 (2013).

[27] *Cf.* Patricia L. Bellia, *WikiLeaks and the Institutional Framework for National Security Disclosures*, 121 YALE L.J. 1448, 1499-1502 (2012) (stating that WikiLeaks' information brokering with multiple newspapers made it impossible for the *New York Times* to delay publication).

[28] *See* Papandrea, *supra* note 3, at 236.

[29] *See, e.g.*, Barton Gellman, Remarks at the Georgetown Journal of National Security Law and Policy Symposium: Leakers, Whistleblowers, and Traitors: An Evolving Paradigm, at 02:47:00 (Feb. 25, 2014), http://apps.law.georgetown.edu/webcasts/eventDetail.cfm?eventID=2275 (arguing that it is "profoundly wrong" to suggest that journalists are indifferent to the risk of prosecution they might face under the Espionage Act and

cannot realistically threaten foreign publishers with prior restraint or ex post criminal prosecution for disseminating particularly dangerous secrets because they operate largely outside of U.S. jurisdiction. Any attempt to enforce a prior restraint against an entity like WikiLeaks would be an exercise in futility. WikiLeaks hosted its content on a complicated web of redundant servers located in a variety of jurisdictions.[30] As the pursuit of Julian Assange demonstrates, extraditing foreigners to the United States to face prosecution for publishing leaks is also extraordinarily difficult.[31]

The Bradley Manning mass document dump illustrates how easily, indiscriminately, and potentially anonymously leakers can reveal the nation's secrets. The costs of gathering and disseminating information to the public (or an intermediary) have diminished to almost zero. While Daniel Ellsberg had to copy each page of the Pentagon Papers painstakingly, Bradley Manning just had to download files onto a flash drive. The internet makes it possible to disseminate information in searchable format throughout the world in a matter of moments. Although Adrian Lamo revealed Manning's identity,[32] and Edward Snowden did not seek anonymity,[33] the government may not be as lucky in the future. Speaking anonymously online becomes easier by the day, and forcing foreign publishers to comply with a subpoena to reveal their sources is difficult. The hope, then, is that severely punishing the identified leakers will deter future leakers.

Indeed, the government's overwhelming desire to stop leaks may have changed its cost/benefit analysis regarding the overall value of leak prosecutions. In the past, government officials pursued few leak prosecutions out of the fear that more harm than good would come from the prosecution; they might have to reveal even more sensitive information in order to demonstrate that the information was properly classified and damaging to U.S. national security interests.[34] So-called "graymail" can still happen – the

related statutes for publishing national security information).

[30] *See* Bellia, *supra* note 27, at 1482-83.

[31] Bill Dedman, *U.S. v. WikiLeaks: Espionage and the First Amendment*, NBC NEWS, http://www.nbcnews.com/id/40653249/ns/us_news-wikileaks_in_security/t/us-v-wikileaks-espionage-first-amendment/#.UwVrNP1td-U (last visited Feb. 8, 2014), *archived at* http://perma.cc/MRK9-DADK.

[32] Kevin Pouslen & Kim Zetter, *U.S. Intelligence Analyst Arrested in WikiLeaks Video Probe*, WIRED (June 6, 2010), http://www.wired.com/threatlevel/2010/06/leak, *archived at* http://perma.cc/VJH8-LXY9.

[33] Glenn Greenwald, *Edward Snowden: The Whistleblower Behind the NSA Surveillance Revelations*, GUARDIAN (June 9, 2013), http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance, *archived at* http://perma.cc/98QS-YUBS (revealing the identity of Edward Snowden as the source of information about NSA surveillance practices "at his request").

[34] *National Security Leaks and the Law: Hearing Before the Subcomm. on Crime, Terrorism, & Homeland Sec. of the H. Comm. on the Judiciary*, 112th Cong. 11 (2012) (statement of Kenneth Wainstein, Homeland Security Advisor) ("[E]ven when investigators

government claimed it dropped its prosecution of Thomas Drake for this reason[35] – but the Classified Information Procedures Act has made it much less likely that the government will have to expose more classified information in order to have a successful prosecution.[36] Furthermore, because improvements to surveillance technologies make it easier to obtain evidence of a defendant's guilt, the risk of graymail is low; indeed, most defendants plead guilty.[37]

Another possible explanation for the rise in leak prosecutions is that the government feels that it has more valuable secrets to protect than in the past. Gabriel Schoenfeld argues that leaks from the founding era were much more innocuous, and much less capable of compromising national security, than more recent leaks regarding methods of fighting global terrorism.[38] Whether today's secrets are that much more valuable is debatable; Dana Priest and William Arkin report that their military and intelligence sources cannot name a single post–September 11 leak that has caused serious harm to national security.[39] Determining whether a particular leak causes harm can be difficult, but what matters is whether the executive branch believes that leaks connected with its counterterrorism efforts are particularly dangerous.

Relatedly, the government may simply be overwhelmed with the number of secrets it is trying to keep. The number of covert and clandestine operations has multiplied.[40] Many of these operations are controversial, leading to a

can get by those challenges and the leaks are identified, the agency whose information was compromised is often reluctant to proceed with a prosecution out of fear that trying the case in public will both highlight the compromised information and disclose further sensitive information that it wants to keep confidential.").

[35] Charlie Savage, *Finding Sources of Leaked Secrets Is Hard; Bringing a Case Is Harder*, N.Y. TIMES, June 10, 2012, at A20. Critics suggest that the government invoked the need to protect classified information as a cover for its desire to drop a weak case, especially given Drake's plan to present testimony from a former classification czar that the information at issue in the case should never have been classified. *See, e.g.*, Isikoff, *supra* note 8.

[36] 18 U.S.C. app. § 3 (2012) ("Upon motion of the United States, the court shall issue an order to protect against the disclosure of any classified information disclosed by the United States to any defendant in any criminal case in a district court of the United States.").

[37] Ann E. Marimow, *Former State Dept. Arms Expert Pleads Guilty in Leak to Fox News Reporter*, WASH. POST, Feb. 8, 2014, at A4 ("[M]ost accused leakers in recent years have pleaded guilty rather than go to trial.").

[38] SCHOENFELD, *supra* note 6, at 82 (stating that the age of global terrorism poses far greater intelligence risks than the "age of musket fire and wind-borne ships").

[39] PRIEST & ARKIN, *supra* note 2, at xx ("Despite all the unauthorized disclosures of classified information and programs in scores of articles since September 11, 2001, our military and intelligence sources cannot think of an instance in which security has been seriously damaged by the release of information."); *see also id.* at 269 ("[L]oss of any particular technology that would have had a severe impact on U.S. capabilities [during the Cold War] would these days likely just prompt a new round of innovation to replace it . . . .").

[40] *Id.* at 12.

greater likelihood of leaks.[41] The digital age has led to the collection of incredible amounts of data, much of which is accessible in digital form (and thus more easily copied and disseminated). The government now struggles to strike the right balance between providing sufficient access to information to those who may need it for work purposes, and concerns that broad access to information will make it harder for the government to control the information. After the September 11 attacks, the 9/11 Commission criticized the government for excessively compartmentalizing information.[42] On the other hand, some critics have lambasted the government for giving too many people access to the nation's secrets, especially after the Manning and Snowden leaks.[43] While insufficient information control poses its own set of risks, excessive secrecy may undermine respect for the classification system.[44] The government might believe that leak prosecutions counteract this loss of respect.

The government often claims that one reason why it has not prosecuted more leakers is that they are difficult to identify.[45] But the prosecution of Jeffrey Sterling,[46] as well as recent revelations regarding the widespread collection of phone records for Associated Press (AP) reporters[47] and the surveillance of Fox's Chief White House Correspondent James Rosen,[48]

[41] *Id.* at 32 (explaining that people have a number of reasons for talking about what they know, including "a desire to correct the record or to explain away something that sounds evil, or to save the agency from itself, or to stop wrongdoing").

[42] *See* NAT'L COMM'N ON TERRORIST ATTACKS UPON THE U.S., THE 9/11 COMMISSION REPORT 417 (2004), *archived at* http://perma.cc/W4LF-GB7Z.

[43] Brad Plumer, *About 500,000 Private Contractors Have Access to Top-Secret Info*, WONKBLOG WASH. POST (June 11, 2013, 11:01 AM), http://www.washingtonpost.com/blogs/wonkblog/wp/2013/06/11/about-500000-private-contractors-have-access-to-top-secret-information, *archived at* http://perma.cc/X7A5-ERQM ("One of the big questions raised after Edward Snowden exposed the NSA's secret surveillance programs is how a private contractor working at Booz Allen Hamilton had access to such sensitive information in the first place.").

[44] Elizabeth Goitein & David M. Shapiro, *Reducing Overclassification Through Accountability*, BRENNAN CENTER FOR JUST. N.Y.U. SCH. L. 7 (Oct. 5, 2011), http://www.brennancenter.org/publication/reducing-overclassification-through-accountability, *archived at* http://perma.cc/5NRW-BVSB ("[O]verclassification erodes government employees' respect for the classification system . . . .").

[45] Adam Liptak, *A High-Tech War on Leaks*, N.Y. TIMES, Feb. 11, 2012, at SR5 ("As a general matter, prosecutions of those who leaked classified information to reporters have been rare, due, in part, to the inherent challenges involved in identifying the person responsible for the illegal disclosure and in compiling the evidence necessary to prove it beyond a reasonable doubt." (quoting a Justice Department official) (internal quotation marks omitted)).

[46] *See* United States v. Sterling, 724 F.3d 482, 489 (4th Cir. 2013).

[47] Savage & Kaufman, *supra* note 10, at A1.

[48] Anne E. Marimow, *Records Offer Rare Glimpse at Leak Probe*, WASH. POST, May 20, 2013, at A1. The government obtained a warrant to search the reporter's personal emails, traced the timing of his phone calls with a State Department security advisor, and combed

illustrate how things have changed. Today, the government can search not only work-related communications devices (even if used for non-work-related purposes),[49] but also email, phone, and travel records from third parties and track the communications and movements of both government insiders and journalists through GPS-enabled cellphones. Even meetings in dark parking garages *à la* Bob Woodward in *All the President's Men* are not safe if a camera captures footage of every person that comes in and out.[50] Journalists report that their government sources have become "reluctant to discuss even unclassified information with them," as these sources are worried about the possibility of a leak investigation based on government surveillance of every email and phone call they make.[51] Advances in surveillance technology not only make it easier for the government to identify leakers without subpoenaing reporters, but also make it more likely that a prosecution will be successful.[52]

To the extent that such action is necessary, the government's reluctance to subpoena a reporter in a leak prosecution has diminished. Since the early 1970s, the Department of Justice (DOJ) has had internal guidelines that prohibit issuing subpoenas to reporters unless other avenues of investigation have been exhausted and the Attorney General expressly grants approval.[53] These guidelines are not binding on the government and do not apply to special prosecutors.[54] As a result, Special Prosecutor Patrick Fitzgerald did not hesitate to subpoena various members of the press during his investigation of the

security badge records to track the reporter's visits to the State Department. *Id.*

[49] *See* Savage & Kaufman, *supra* note 10, at A1. A lawsuit has been filed based on the admitted practice of the Food and Drug Administration (FDA) of accessing employees' private email accounts accessed on work computers; the agency also reviewed documents stored on government-issued computer and took electronic screen shots of computer desktops. Ellen Nakashima & Lisa Rein, *FDA Says It Monitored E-Mails to Investigate Leaks*, WASH. POST, Feb. 10, 2012, at A18.

[50] Liptak, *supra* note 45. Concerns that the government is conducting surveillance of reporters has led many journalists to become experts in encryption and other tools to protect the security of communications with their sources. *See, e.g.*, Lauren Kirchner, *Encryption, Security Basics for Journalists*, COLUM. JOURNALISM REV. (Sept. 17, 2013, 2:50 PM), http://www.cjr.org/behind_the_news/hacks_hackers_security_for_jou.php?utm_source=dlvr.it&utm_medium=twitter, *archived at* http://perma.cc/JNS6-WHVC; Amy Zhang, *Whistleblowers to Journalists: Protect Your Data*, NEWS MEDIA & L., Summer 2013, at 3.

[51] *See* Leonard Downie, Jr., *Special Report: The Obama Administration and the Press: Leak Investigations and Surveillance in Post-9/11 America*, COMM. TO PROTECT JOURNALISTS (Oct. 10, 2013), http://cpj.org/reports/2013/10/obama-and-the-press-us-leaks-surveillance-post-911.php, *archived at* http://perma.cc/89LV-PVDD.

[52] *Id.*

[53] *See* Branzburg v. Hayes, 408 U.S. 665, 707 n.41 (1972).

[54] *In re* Special Proceedings, 373 F.3d 37, 44 n.3 (1st Cir. 2004) ("The regulation states that 'the following guidelines shall be adhered to by all members of the Justice Department in all cases,' 28 C.F.R. § 50.10 (2003), but a special prosecutor is not a member of the Justice Department.").

Valerie Plame leaks, and a *New York Times* reporter ended up spending eighty-five days in jail.[55] Perhaps as a result of the Plame case, prosecutors subject to DOJ regulations appear less reluctant to subpoena reporters and third parties holding their records. In May 2013, it was revealed that DOJ issued sweeping subpoenas for the phone records of AP reporters without prior notification[56] and obtained a warrant for the phone and email records of White House correspondent James Rosen of Fox News on the grounds that he had "aided and abetted" a leak.[57] In addition, Holder approved the subpoena of *New York Times* reporter James Risen in the Jeffrey Sterling prosecution, and won a big victory when the Fourth Circuit denied Risen's motion to quash.[58] Although DOJ just revised its internal guidelines regarding media investigations in response to the recent controversies,[59] it also said "leaks of classified information to the press can pose a serious risk of harm to our national security and it is important that we pursue these matters using appropriate law enforcement tools."[60]

DOJ may also feel emboldened to subpoena reporters in light of weakening judicial support for a reporter's privilege, especially in leak cases.[61] In addition, Congress has shown little interest in protecting journalists in leak investigations. Although thirty-nine states and the District of Columbia have statutory shield laws, the frequent efforts to pass a federal shield law have failed.[62] The WikiLeaks disclosures derailed a bill approved by the Senate Judiciary Committee in 2009; ultimately, the bill never reached a vote in the

[55] Michael Calderone, *Times' Abramson Is on—Then off! in Scooter Trial*, N.Y. OBSERVER, Feb. 19, 2007, at 1.

[56] *See* Sari Horwitz, *Justice Dept. Seized Phone Records of AP Journalists*, WASH. POST, May 14, 2013, at A1.

[57] Calderone & Reilly, *supra* note 11.

[58] Shane & Savage, *supra* note 7.

[59] DOJ, REPORT ON REVIEW OF NEWS MEDIA POLICIES 1 (2013), *archived at* http://perma.cc/8G8U-SX8C.

[60] *Justice Department Affidavit Labels Fox News Journalist as Possible 'Co-Conspirator,'* FOX NEWS (May 30, 2013), http://www.foxnews.com/politics/2013/05/20/justice-department-obtained-records-fox-news-journalist, *archived at* http://perma.cc/ZW4F-XYSR. Indeed, in announcing that Donald Sachtleben had plead guilty to leaking information to AP about a foiled bombing plot in Yemen, DOJ made clear that the phone record search was critical in identifying him as the source of the unauthorized disclosure. Savage, *supra* note 18.

[61] *See, e.g.*, United States v. Sterling, 724 F.3d 482, 492, 499 (4th Cir. 2013) (holding that there is no First Amendment or federal common law protection for a reporter's privilege); McKevitt v. Pallasch, 339 F.3d 530, 535 (7th Cir. 2003) (holding that the First Amendment did not provide privilege for a reporter).

[62] *Legislative Protection of News Sources*, REPORTERS COMM., http://www.rcfp.org/first-amendment-handbook/introduction-legislative-protection-news-sources-constitutional-privilege-a (last visited Nov. 13, 2013), *archived at* http://perma.cc/YPN5-J7U3.

full Senate.[63] Although DOJ says that it supports a shield bill, the government has been careful to push for legislation that would offer little protection to reporters in national security leak investigations.[64]

To be sure, the government is still not prosecuting every leak. This selective prosecution is arguably part of the problem.[65] One researcher who has interviewed many active and retired CIA officials reports that the agency "selectively enforces its edicts on secrecy, using different standards depending on rank, message, internal politics and whim."[66] As tempting as it is to argue that the government prosecutes only those who leak embarrassing or negative information, it is not clear that the government's track record during the last decade would actually support this argument. The government has declined to prosecute many leaks, including some significantly damaging ones.[67]

Nevertheless, even if the increase in leak prosecutions is largely accidental, the Obama Administration has clearly made a commitment to prosecute leakers aggressively, and journalists claim these prosecutions are having the desired effect of chilling the willingness of government insiders to share information with them. *New York Times* national security reporter Scott Shane reports that "[g]overnment officials who might otherwise discuss sensitive topics will refer to these cases in rebuffing a request for background

[63] Charlie Savage, *Criticized on Seizure of Records, White House Pushes Media Shield Law*, N.Y. TIMES, May 15, 2013, at A19.

[64] David Stout, *After Debating Definition of 'Journalist,' Senate Panel Passes Shield Law*, MAIN JUST. (Sept. 12, 2013), http://www.mainjustice.com/2013/09/12/after-debating-definition-of-journalist-senate-panel-passes-shield-law, *archived at* http://perma.cc/W2F8-6VQ2 (stating that both President Obama and DOJ supported the Free Flow of Information Act, a bill that would put into law "recently revised Department of Justice guidelines for investigations involving journalists and information pertaining to national security"). The proposed legislation has a national security exception for criminal investigations or prosecutions of "allegedly unlawful disclosure of properly classified information" when compelled disclosure would "materially assist" the Department of Justice "in preventing or mitigating . . . (i) an act of terrorism; or (ii) other acts that are reasonably likely to cause significant and articulable harm to national security." Free Flow of Information Act, S. 987, 113th Cong. § 5(a)(2)(A) (2013). Critics complain that this exception will essentially eliminate protection for national security reporters in most instances. *See* David Freedlander, *Media Balks at Band-Aid Shield Law*, DAILY BEAST (May 16, 2013), http://www.thedailybeast.com/articles/2013/05/16/media-balks-at-band-aid-shield-law.html, *archived at* http://perma.cc/FXK5-3UQV.

[65] The same could be said for the government's prepublication clearance requirements; some books by former employees are subject to extensive redactions; others sail through with the government's blessing.

[66] Ted Gup, *Secrecy Double Standard*, N.Y. TIMES, Jan. 9, 2013, at A21.

[67] *See* Pozen, *supra* note 26 (detailing the government's failure to prosecute leaks aggressively); *see also* SCHOENFELD, *supra* note 6, at 239 (arguing that the low numbers of leak prosecutions "does not exactly constitute a reign of terror"); Richard Moberly, *Whistleblowers and the Obama Presidency: The National Security Dilemma*, 16 EMPLOYEE RTS. & EMPL. POL'Y J. 51, 80 n.177 (2012).

information."[68] He believes the recent uptick in leak prosecutions has "definitely [had] a chilling effect" on the willingness of government insiders to talk to reporters.[69] This effect has also taken hold of some journalists who are afraid to publish stories likely to lead to a subpoena, and potential jail time and crippling fines if they refuse to testify.[70]

Despite President Obama's proclaimed commitment to government transparency,[71] critics complain that his presidency is "turning out to be the administration of unprecedented secrecy and of unprecedented attacks on a free press."[72] In addition to chilling discussions between the press and government officials, this Administration has been much less willing than prior administrations to discuss sensitive information with reporters.[73] Journalists claim that designated spokespersons "are often unresponsive or hostile to press inquiries, even when reporters have been sent to them by officials who won't talk on their own."[74] Another common concern is that the crackdown on leaks, and the executive branch's desire to exercise tight control over the flow of information to the media, has chilled all unauthorized disclosures, not just those involving classified or otherwise sensitive information.[75] The recently established Insider Threat Program encourages government insiders to report their coworkers' suspicious conduct and to monitor "indicators" that suggest they may leak information, including "stress, divorce, and financial problems."[76] One reporter observed that journalists often talk to their

[68] Margaret Sullivan, Op-Ed., *The Danger of Suppressing the Leaks*, N.Y. TIMES, Mar. 10, 2013, at SR12.

[69] *Id.*

[70] RonNell Anderson Jones, *Media Subpoenas: Impact, Perception, and Legal Protection in the Changing World of American Journalism*, 84 WASH. L. REV. 317, 393-94 (2009) (stating that the upswing in subpoenas has spurred "a wave of terror in journalism that is leading even those who have not been subpoenaed to limit their news coverage"). I have also had off-the-record conversations with reporters who have told me that they are sometimes reluctant to publish information that their sources willingly provide because they are concerned about what will happen to their sources as a result of their disclosures.

[71] Transparency and Open Government: Memorandum for the Heads of Executive Departments and Agencies, 74 Fed. Reg. 4685, 4685 (Jan. 26, 2009) ("My Administration is committed to creating an unprecedented level of openness in Government.").

[72] Margaret Sullivan, Op-Ed., *Leak Investigations Are an Assault on the Press, and on Democracy, Too*, N.Y. TIMES (May 14, 2013, 5:40 PM), http://publiceditor.blogs.nytimes.com/2013/05/14/leak-investigations-are-an-assault-on-the-press-and-on-democracy-too, *archived at* http://perma.cc/4ENM-3WEG. Not surprisingly, Administration officials disagree with this characterization. *See* Downie, Jr., *supra* note 51.

[73] Downie, Jr., *supra* note 51.

[74] *Id.* According to Downie, Chief Washington Correspondent for the *New York Times* David E. Sanger claims that "[t]his is the most closed, control freak administration I've ever covered." *Id.*

[75] *Id.*

[76] *Id.*; Taylor & Landay, *supra* note 2 (reporting that experts and current and former

government sources through third-party intermediaries "so the sources can truthfully answer on polygraphs that they didn't talk to reporters."[77]

These measures are not likely to prevent all leaks, but are likely primarily affecting those that undermine the executive branch's agenda. The executive's control over national security information includes its power to leak – or "plant" – information when it suits its purposes.[78] As I detail extensively elsewhere,[79] Presidents commonly use leaks (or plants) to serve their own agendas. Indeed, the majority of leaks appear to come not from disgruntled employees or contractors but from high-level government officials – the "ship of state is the only ship that leaks from the top."[80] It is also important to keep in mind that these leaks often concern the military, national security, and foreign affairs.[81] The rise in leak prosecutions may therefore distort public debate by primarily discouraging leaks from lower-level employees critical of those in power.

B. *The Imperfect Role of Leaks*

Leaks play an essential, yet imperfect, role in checking executive power and informing the American public about the government's policies and programs. The "name game" in the public discourse of characterizing leakers as traitors, spies, or whistleblowers reflects the unease with which Americans view leakers, as well as the fuzzy lines that separate each category.

1. Checks and Balances

The executive branch needs some control over the dissemination of national security information in order to conduct effective military actions, foreign policy, and diplomatic relations. In some instances, the disclosure of national security information outside of the executive branch can pose a genuine threat to our nation's national security.[82] Although the Constitution makes little mention of secrecy,[83] the Framers certainly recognized that some governing

officials predict that the Insider Threat Program "could make it easier for the government to stifle the flow of unclassified and potentially vital information to the public, while creating toxic work environments poisoned by unfounded suspicions and spurious investigations of loyal Americans").

[77] Downie, Jr., *supra* note 51 (quoting *Washington Post* National Editor Cameron Barr).

[78] Papandrea, *supra* note 3, at 248-57.

[79] *Id.* at 248-55.

[80] *Id.* at 253.

[81] *Id.*

[82] United States v. Curtiss-Wright Exp. Corp., 299 U.S. 304, 320 (1936) (describing the importance of secrecy in the executive branch).

[83] The only mention of secrecy is in Article I, in a provision requiring the House and Senate to keep journals of their proceedings and to publish them "from time to time . . . excepting such Parts as may in their Judgment require Secrecy . . . ." U.S. CONST. art. I, § 5, cl. 3.

must take place outside of the public eye to be effective.[84] The problem is that the Framers "did not fully explain how citizens and lawmakers could know whether the president is in fact exercising this power responsibly."[85] Various reforms in the last several decades, including the passage of the Freedom of Information Act and the creation of congressional oversight committees, have failed to serve as significant counterweights to the executive's ability to control the flow of national security information.[86] Since September 11, the Bush and Obama Administrations have both aggressively asserted their power to control the dissemination of national security information and undermined the checking function of Congress and the judiciary.[87]

The very nature of the executive branch's duties and responsibilities makes true transparency and accountability difficult. The executive is charged with "executing" the law, and the vast administrative state enables the execution of many laws to transpire in the dark.[88] The difficulties of monitoring the executive are exponentially greater whenever national security is involved. The executive exercises tight control over national security information through the classification system; the assertion of the executive and state secrets privileges; and general assertions time and time again that the executive has the power to keep information from Congress whenever disclosure would harm foreign relations, national security, or the executive's deliberative processes or constitutional duties.[89] The executive branch has repeatedly asserted its power to control the dissemination of national security information during battles with Congress over Congress's efforts to exercise some meaningful oversight of presidential power.[90]

---

[84] Papandrea, *supra* note 3, at 239 ("For example, Alexander Hamilton said that the Constitution would not have been ratified if the Convention had been open to the public because 'the clamours of faction would have prevented any satisfactory result.'" (quoting Alexander Hamilton, *Reply to Anonymous Charges*, *in* 3 THE RECORDS OF THE FEDERAL CONVENTION 1787, at 368 (Max Farrand ed., 1966))).

[85] RAHUL SAGAR, SECRETS AND LEAKS 49 (2013).

[86] *Id.* at 46-50.

[87] *See* HEIDI KITROSSER, RECLAIMING ACCOUNTABILITY (forthcoming 2015) (manuscript at 3) (on file with author); CHARLIE SAVAGE, TAKEOVER: THE RETURN OF THE IMPERIAL PRESIDENCY AND THE SUBVERSION OF AMERICAN DEMOCRACY 237 (2007); GARRY WILLS, BOMB POWER: THE MODERN PRESIDENCY AND THE NATIONAL SECURITY STATE 210-20 (2010); Neal Devins, *Presidential Unilateralism and Political Polarization: Why Today's Congress Lacks the Will and the Way to Stop Presidential Initiatives*, 45 WILLAMETTE L. REV. 395, 399-400 (2009); William P. Marshall, *Eleven Reasons Why Presidential Power Inevitably Expands and Why It Matters*, 88 B.U. L. REV. 505, 511-18 (2008).

[88] *See* KITROSSER, *supra* note 87 (manuscript at 3).

[89] *See* Heidi Kitrosser, *National Security and the Article II Shell Game*, 26 CONST. COMMENT. 483, 519 (2010).

[90] Moberly, *supra* note 67, at 82-83 (detailing the House's efforts to provide protection to whistleblowers who leak national security information, and the executive's opposition to the measures, despite previous expressions of support for similar measures).

Although Congress sometimes appears to accept the executive's assertions of national security power without putting up much of fight or exercising meaningful oversight,[91] Congress generally disputes the executive's theory of the separation of powers. Instead, Congress contends that it shares authority over national security matters with the executive.[92] Congress has a number of tools at its disposal to encourage disclosures – for example, it can conduct hearings, subpoena testimony and documents, leverage its power in the appropriations and appointments process, and pass statutes that require periodic reports from the executive branch. The executive, however, strongly resists Congress's attempts to force the disclosure of information, and there is very limited opportunity for judicial review of these interbranch disputes.[93] Congress has not been particularly effective in forcing the executive to reveal national security information.[94]

Even when the executive is willing to share information regarding its national security initiatives, it generally does so with only a select group of congressional members, and the executive may – or may not – share all of the relevant details of its programs with these select members.[95] Those members who do have access to information about the President's activities may feel they have no meaningful way of voicing their concerns about them.[96] While some have argued that the Constitution's Speech and Debate Clause would immunize from prosecution disclosures of national security information a member might make on the House or Senate floor,[97] such disclosures would

[91] PRIEST & ARKIN, *supra* note 2, at 23 (explaining that Congress's failure to exercise meaningful oversight is not always just "a matter of money and staff," but rather that Congress sometimes simply takes the President at his word without "studying the best information available or conducting exhaustive hearings"); *see also* SAGAR, *supra* note 85, at 94-98 (outlining several possible reasons why secretive oversight committees provide generally ineffective oversight of the executive branch).

[92] *See* LOUIS FISHER, CONG. RESEARCH SERV., RL33215, NATIONAL SECURITY WHISTLEBLOWERS 41 (2005), *archived at* http://perma.cc/7T9G-EUZM ("Congress has never accepted the theory that the President has exclusive, ultimate, and unimpeded authority over the collection, retention, and dissemination of national security information.").

[93] KITROSSER, *supra* note 87.

[94] *See* Moberly, *supra* note 67, at 96-101.

[95] *See* Shirin Sinnar, *Protecting Rights from Within? Inspectors General and National Security Oversight*, 65 STAN. L. REV. 1027, 1083 (2013); Nathan Freed Wessler, *"[We] Can Neither Confirm Nor Deny the Existence or Non-Existence of Records Responsive to Your Request": Reforming the Glomar Response Under FOIA*, 85 N.Y.U. L. REV. 1381, 1390 (2010).

[96] SAGAR, *supra* note 85, at 95 (arguing that limiting the disclosure of national security information to a select group of members of Congress leaves those members "unable to explain to the public why they wish to block or investigate the president's policies or decisions").

[97] *See, e.g.*, Bruce Ackerman, *Breach or Debate*, FOREIGN POL'Y (Aug. 1, 2013), http://

violate House and Senate procedures regarding the release of classified information obtained from the executive branch.[98] Although Congress could certainly repeal these rules, it is not clear it would be wise to do so. It is likely that at some point a member would reveal information that causes serious national security harm; in addition, a relaxation of these rules could give the President another justification for refusing to share information with Congress.[99]

The executive's disclosures to Congress may also be misleading, incomplete, or even false. For example, in March 2013 Senator Ron Wyden directly asked James Clapper, the Director of National Intelligence: "[D]oes the NSA collect any type of data at all on millions, or hundreds of millions, of Americans?"[100] Clapper stated that the government did not collect such data, at least "not wittingly."[101] After the Snowden leaks made clear that this response was false, Clapper explained that his response was the "least untruthful" answer he could give when asked about a classified program in an open session.[102] Concerned about the failure of intelligence agencies to provide full

www.foreignpolicy.com/articles/2013/08/1/breach_or_debate_congress_snowden_prism, *archived at* http://perma.cc/K4NX-RT7Q (arguing members of select intelligence committees "cannot be prosecuted for reading classified material into the public record– and it is up to them, and them alone, to decide what is worth talking about"); *see also* United States v. Gravel, 408 U.S. 606, 616 (1972).

[98] *See* Michael Stern, *Congressional Release of Classified Information and the Speech and Debate Clause*, POINT ORDER (Aug. 6, 2013), http://www.pointoforder.com/2013/08/06/congressional-release-of-classified-information-and-the-speech-or-debate-clause, *archived at* http://perma.cc/G6ZD-X5WV.

[99] *Id.*

[100] *Current and Projected National Security Threats to the United States: Hearing Before the S. Select Comm. on Intelligence*, 113th Cong. 66 (2013) (statement of Sen. Ron Wyden, Member, S. Select Comm. on Intelligence).

[101] *Id.* (statement of James R. Clapper, Director of National Intelligence).

[102] Interview by Andrea Mitchell with James Clapper, Dir. of Nat'l Intelligence (June 8, 2013) (transcript archived at http://perma.cc/SJF4-FJ7K). Some contend that Clapper could not have misled the Senate Select Committee on Intelligence because members of that committee already knew about the collection of information about Americans. *See* Steven Aftergood, *The Clapper "Lie," and the Senate Intelligence Committee*, SECRECY NEWS (Jan. 6, 2014), http://blogs.fas.org/secrecy/2014/01/clapper-ssci, *archived at* http://perma.cc/3MK3-9TB8. Members of Congress disagree about how much knowledge and information they had about NSA's surveillance programs. *See* Scott Shane & Jonathan Weisman, *Disclosures on N.S.A. Surveillance Put Awkward Light on Previous Denials*, N.Y. TIMES, June 12, 2013, at A18; *see also In Re* Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [Redacted] 3, No. BR 13-158 (Foreign Intelligence Surveillance Ct.), *archived at* http://perma.cc/6NBT-MF9F ("Although the existence of this [collection of metadata under section 215] was classified until several months ago, the record is clear that before the 2011 re-enactment of Section 215, many Members of Congress were aware of, and each Member had the opportunity to learn about, the scope of the metadata collection and this Court's interpretation of Section 215.").

and accurate information to Congress, Senator John McCain has submitted a resolution to establish a select committee to investigate NSA's intelligence-collecting programs, including "the provision of incomplete or inaccurate information by officials of the intelligence community [that] has inhibited effective congressional oversight" of those programs.[103]

Given how tightly the executive branch attempts to control the dissemination of national security information, it is no surprise that leaks have played an important role in informing Congress about what its co-branch of government is doing.[104] A member of the Senate Intelligence Committee has said, "I can recall numerous specific instances where I found out about serious government wrongdoing – such as NSA's warrantless wiretapping program, or the CIA's coercive interrogation program – only as a result of disclosures by the press."[105] The Snowden leaks regarding the mass collection of communications metadata similarly appear to have told Congress how the executive was executing the law.[106] When the *Guardian* revealed that the government had ordered Verizon to collect information on all of its customers' calls,[107] Congressman F. James Sensenbrenner, Jr. stated:

> As the author of the Patriot Act, I am extremely disturbed by what appears to be an overbroad interpretation of the Act. . . . I do not believe the released FISA order is consistent with the requirements of the Patriot Act. How could the phone records of so many innocent Americans be relevant to an authorized investigation as required by the act?[108]

Another particular concern about government surveillance is the inability of congressional leaders to understand what the government is doing. The few congresspersons with access to information about the government's inventive and expansive use of technology to spy on millions of people are generally not

---

[103] 160 CONG. REC. S765-67 (daily ed. Feb. 4, 2014) (statement of Sen. John McCain); *see also* S. Res. 343, 113th Cong. (2014).

[104] SAGAR, *supra* note 85, at 48 ("To the extent that citizens and lawmakers have become aware of potential wrongdoing in the past decade—the establishment of secret prisons, the practice of extraordinary rendition, and the existence of warrantless surveillance programs—this has been due to unauthorized disclosures.").

[105] 158 CONG. REC. S6793-94 (daily ed. Nov. 14, 2012) (statement of Sen. Ron Wyden).

[106] James Risen, *Bipartisan Backlash Grows Against Domestic Surveillance*, N.Y. TIMES, July 17, 2013, at A14.

[107] Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, GUARDIAN (June 5, 2013), http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order, *archived at* http://perma.cc/64ZM-P5ZG.

[108] Letter from F. James Sensenbrenner, Jr., U.S. Congressman, to Eric H. Holder, Jr., U.S. Attorney Gen. (June 6, 2013), *archived at* http://perma.cc/6S5L-LJW6. In September 2013, Congressman Sensenbrenner wrote a second letter to Holder expressing his displeasure. Letter from F. James Sensenbrenner, Jr., U.S. Congressman, to Eric H. Holder, Jr., U.S. Attorney Gen. (Sept. 6, 2013), *archived at* http://perma.cc/HT7W-6CHK.

"child[ren] of the digital age."[109] The few members of Congress and Senators who are given access to highly classified national security activities are not permitted to speak with their lawyers or staff about the issues these programs raise, even if those individuals have the requisite security clearances.[110] Indeed, although the national security state has dramatically expanded since September 11, the support staff numbers for Congress's intelligence committees has not grown much at all.[111] As a result, "members of Congress were left on their own to make sense of highly technical issues."[112] Leaks and the accompanying media analysis help government officials within the political branches do their job better.[113]

Even when Congress knows what the executive is doing, it has been generally deferential to the executive's claims of expansive power in the national security realm.[114] Part of this phenomenon stems from the political party system and the unwillingness of congresspersons to challenge actions taken by Presidents from the same political party.[115] But experience indicates that congressional oversight is not much more effective even when the executive and legislative branches are controlled by different parties.[116] Furthermore, as Heidi Kitrosser has observed, "ignorance can be bliss."[117] When unaware of what the executive is doing, Members of Congress can easily distance themselves from any public outcry that might ensue when those

[109] Alan Rusbridger, *The Snowden Leaks and the Public*, N.Y. REV. BOOKS, Nov. 21, 2013, at 31, 33.

[110] PRIEST & ARKIN, *supra* note 2, at 23.

[111] *Id.* at 22.

[112] *Id.* at 23.

[113] *See* Blasi, *supra* note 13, at 539 ("Moreover, even with their own investigative resources, government officials engaged in the process of checking other public officials often benefit from the work of journalists and private citizens.").

[114] For example, although Congress resorted to holding up the confirmation of President Obama's nominees for the CIA and Department of Defense until the President provided Congress with the legal memoranda justifying drone attacks, Congress capitulated after receiving redacted copies. *See* Scott Shane, *Nominee to Lead C.I.A. Clears Hurdle After Release of Drone Data*, N.Y. TIMES, Mar. 6, 2013, at A13; *see also* Martha Minow, *The Constitution as Black Box During Emergencies*, 75 FORDHAM L. REV. 593, 597-98 (2006) (arguing that the U.S. experience after 9/11 reveals the failure of Congress to provide meaningful oversight of the executive in the face of terrorism).

[115] *See* Daryl J. Levinson & Richard H. Pildes, *Separation of Parties, Not Powers*, 119 HARV. L. REV. 2312, 2313-14, 2323, 2344 (2006) ("[P]arties can – and often do – change the relationship between Congress and the President from competitive to cooperative.").

[116] *See, e.g.*, SAGAR, *supra* note 85, at 97 ([C]oncerns about the quality of oversight do not fade away *even when* a majority of the members of the core [oversight] group come from the party opposed to the president."); Minow, *supra* note 114, at 598 (arguing that the Democrats' resistance to NSA's secret surveillance programs during the Bush Administration was "flabby").

[117] KITROSSER, *supra* note 87 (manuscript at 6).

activities are revealed. In addition, challenging the executive's national security policies opens congresspersons up to criticism, such as accusations that they are not tough on terrorism, and the professional staff of the oversight committees tends to consist disproportionately of former intelligence community employees. Although these individuals bring important expertise to their jobs, they have not devoted their careers to "civil liberties, government accountability, or personal privacy."[118] The realities of the political process may also limit the effectiveness of congressional oversight because elected officials cannot engage in any "inside baseball" discussions about the congressional intelligence committee's work with potential donors.[119]

More cynically, as the national security state continues to expand and depend on government contractors, federal lawmakers are coming to rely on significant campaign donations from these contractors.[120] As a result, many senators and representatives will find it does not serve their political self-interest to exercise meaningful oversight over these contractors. Indeed, after the House narrowly defeated a bill to restrict NSA's spying program, a study revealed that those who voted against the bill received twice as much in campaign donations from defense contractors as those who voted in favor of the law.[121] It is hard to view this as a coincidence.

Legislative attempts to counteract excessive secrecy have been minimally effective. The Freedom of Information Act (FOIA), as well as other federal laws providing for the disclosure of government information,[122] exempt properly classified national security secrets from disclosure.[123] Generally

[118] Steven Aftergood, *A Candid Look at the Senate Intelligence Committee*, SECRECY NEWS (June 18, 2013), http://blogs.fas.org/secrecy/2013/06/ssci-candid, *archived at* http://perma.cc/DYB4-8EMH.

[119] JACK GOLDSMITH, POWER AND CONSTRAINT: THE ACCOUNTABLE PRESIDENCY AFTER 9/11, at 91 (2012).

[120] *See* Ken Heanley, *Big Campaign Donations from Contractors Doing Secret Work for NSA*, DIGITAL J. (June 22, 2013), http://digitaljournal.com/article/352922, *archived at* http://perma.cc/TE4T-R9NH.

[121] *See* David Kravets, *Lawmakers Who Upheld NSA Phone Spying Received Double the Defense Industry Cash*, WIRED (July 26, 2013, 4:14 PM), http://www.wired.com/threatlevel/2013/07/money-nsa-vote, *archived at* http://perma.cc/DL98-BCM3.

[122] *See, e.g.*, Government in the Sunshine Act, 5 U.S.C. § 552b(c)(1) (2012) (preventing disclosure of properly classified information); Privacy Act, 5 U.S.C. § 552a(k)(1) (exempting properly classified material from normal agency disclosure requirements); Federal Advisory Committee Act, 5 U.S.C. app. § 10(b) (mandating that advisory subcommittees make their information available to the public); Administrative Procedure Act, 5 U.S.C. § 553 (2012) (requiring notice to the public of certain types of agency rules); National Environmental Policy Act, 42 U.S.C. § 4332(2)(C) (2006) (instructing agencies to make public information concerning potential environmental effects from federal actions); Paperwork Reduction Act, 44 U.S.C. § 3501(2) (2006) (stating that one purpose of the Act is to promote the public interest by revealing government information).

[123] 5 U.S.C. § 552(b)(1). Exemption 3 provides that the FOIA does not apply to

unwilling to second-guess classification decisions, the Court has often deferred to the executive branch's claims that disclosure of the desired information would harm national security.[124] The Court's decision in *Holder v. Humanitarian Law Project* indicates that the Court is just as likely as ever to defer to the executive branch in national security affairs.[125]

In addition to the tremendous amount of time, money, and patience that FOIA litigation takes, interested citizens cannot make a FOIA request to a government agency involved in national security seeking access to any information concerning "misconduct that has been improperly classified."[126] Instead, the requesters have to have some idea what they are looking for. As a result, requesters frequently only initiate FOIA litigation after leaks have already provided initial revelations about the activity. For example, the abuses at Abu Ghraib came to light only after portions of the Taguba Report were leaked to the media; even after a firestorm of congressional activity, the executive was not forthcoming until additional leaks provided documentation to support the initial allegations.[127]

information that is exempted from disclosure under a separate statute. *Id.* § 552(b)(3). These separate statutory exemptions often raise national security issues. In addition, the FOIA specifically permits the Federal Bureau of Investigation (FBI) to exercise its discretion in determining whether to disclose documents that "pertain[] to foreign intelligence or counterintelligence, or international terrorism," provided these documents constitute "classified information as provided in subsection (b)(1)." *Id.* § 552(c)(3).

[124] *See, e.g.*, Larson v. Dep't of State, 565 F.3d 857, 864 (D.C. Cir. 2009) ("[A reviewing court must] accord substantial weight to an agency's affidavit concerning the details of the classified status of the disputed record because the Executive departments responsible for national defense and foreign policy matters have unique insights into what adverse affects [sic] might occur as a result of a particular classified record." (alteration in original) (quoting Ctr. for Nat'l Sec. Studies v. DOJ, 331 F.3d 918, 927 (D.C. Cir. 2003)) ((internal quotation marks omitted))). For a lengthy discussion of the judiciary's failure to provide meaningful review of classification decisions, see SAGAR, *supra* note 85, at 55-65.

[125] The Court said:

> [W]hen it comes to collecting evidence and drawing factual inferences in [cases implicating national security and foreign policy concerns], "the lack of competence on the part of courts is marked," and respect for the Government's conclusions is appropriate.
>
> One reason for that respect is that national security and foreign policy concerns arise in connection with efforts to confront evolving threats in an area where information can be difficult to obtain and the impact of certain conduct difficult to assess.

Holder v. Humanitarian Law Project, 130 S. Ct. 2705, 2727 (2010) (citation omitted) (quoting Rostker v. Goldberg, 453 U.S. 57, 65 (1981)).

[126] Elizabeth Goitein, *Our Antiquated Laws Can't Cope with National Security Leaks*, TIME (June 12, 2013), http://ideas.time.com/2013/06/12/our-antiquated-laws-cant-cope-with-national-security-leaks, *archived at* http://perma.cc/SRQ7-E4XT.

[127] *See* Seymour M. Hersh, *Torture at Abu Ghraib*, NEW YORKER, May 10, 2004, at 42 (describing the role of leaks to the media in bringing to light improper activity at a military prison in Iraq).

One of the brightest spots in the sad story of the rampant overclassification of national security information is the Interagency Security Classification Appeals Panel (ISCAP). Both government insiders with authorized access to classified information as well as members of the general public can ask the ISCAP to review the classification of information.[128] As Steven Aftergood has proclaimed, the ISCAP "is among the most successful classification reform initiatives of the last half century."[129] The ISCAP's record is impressive: it "has overturned more executive branch classification decisions than any court or legislative action."[130] According to the most recent government report, the panel has declassified information in almost sixty-five percent of its decisions since 1996.[131] The ISCAP arguably provides a more effective means of obtaining national security information from the government than FOIA because FOIA court appeals are time consuming, expensive, and usually unsuccessful given judicial deference to the executive on national security matters.[132] Aftergood has suggested that the success of the ISCAP is due to its ability to eliminate the bureaucratic and political uses of secrecy.[133] In addition, because the members of the ISCAP are all executive branch officials from national security agencies, concerns about deferring to the judgment of the executive are nonexistent.[134]

Although the ISCAP has certainly declassified a significant percentage of the information it has reviewed, it lacks the staff to review more than several dozen requests each year.[135] The lack of a robust staff to deal with the increasing number of appeals, larger systemic issues of overclassification, and the possibility for agencies to appeal the panel's decision remain significant challenges.[136] To date, the ISCAP has also largely dealt with declassification requests from historians and has spent little time on more current classification

[128] Exec. Order No. 13,526 § 1.8, 3 C.F.R. 298, 303 (2010).

[129] Steven Aftergood, *Roslyn Mazer to Be ODNI Inspector General*, SECRECY NEWS (Apr. 6, 2009), http://www.fas.org/blog/secrecy/2009/04/mazer_odni_ig.html, *archived at* http://perma.cc/382L-KZ83.

[130] Steven Aftergood, *National Security Secrecy: How the Limits Change*, 77 SOC. RES. 839, 848 (2010).

[131] INFO. SEC. OVERSIGHT OFFICE, NAT'L ARCHIVES & RECORDS ADMIN., 2011 REPORT TO THE PRESIDENT 23 (2012), *archived at* http://perma.cc/J7BA-3EXB.

[132] Nate Jones, *The CIA's Covert Operation Against Declassification Review and Obama's Open Government*, UNREDACTED (Feb. 10, 2012), http://nsarchive.wordpress.com/2012/02/10/the-cias-covert-operation-against-declassification-review-and-obamas-open-government, *archived at* http://perma.cc/J2VX-MZAZ.

[133] Steven Aftergood, *Reducing Government Secrecy: Finding What Works*, YALE L. & POL'Y REV. 399, 407-09 (2009).

[134] *See* Steven Aftergood, *An Inquiry into the Dynamics of Government Secrecy*, 48 HARV. C.R.-C.L. L. REV. 511, 526 (2013).

[135] *Id.* at 527.

[136] Aftergood, *supra* note 133, at 407-08.

issues.[137] Furthermore, the ISCAP does not consider the public's interest in the information at issue, nor does it balance that interest against the potential harm of disclosure.

Perhaps Congress's most significant exercise of its oversight powers has come through the creation of independent inspectors general. Congress passed the first inspector general (IG) legislation in 1978 to "promote economy, efficiency, and effectiveness" in agency programs and to "prevent and detect fraud and abuse."[138] IGs have played an important role in increasing transparency, arguing for reform, and pushing for accountability.[139] Nevertheless, the ability of IGs to check executive power suffers from significant limitations; importantly, IGs are appointed and removable by the President, and they cannot report even serious wrongdoing to Congress without first giving the relevant agency head the opportunity to delete sensitive information.[140] It might therefore come as no surprise that the CIA's IG has never exposed major wrongdoing within the agency that would have otherwise gone unexposed.[141] Notably, the CIA IG's major investigations all involved matters first revealed by leaks to the press.[142]

If the public does not know what the government is doing in the public's name, accountability is impossible. Without proper public debate, government officials are more likely to adopt ill-conceived programs or policies.[143] Subjecting government action to public discussion and oversight also may make government officials more reluctant to engage in wrongdoing in the first place.[144] Secrecy provides cover for waste, fraud, and illegal actions,[145] and

[137] *See* Aftergood, *supra* note 134, at 527.

[138] Inspector General Act of 1978, 5 U.S.C. app. § 2(2) (2012).

[139] Sinnar, *supra* note 95, at 1043.

[140] *See* Moberly, *supra* note 67, at 93. If an agency head blocks an IG investigation, he must submit a report within seven days to the intelligence committee and to the IG explaining the decision. 50 U.S.C. § 403q(b)(4) (2006).

[141] Ryan M. Check & Afsheen John Radsan, *One Lantern in the Darkest Night: The CIA's Inspector General*, 4 J. NAT'L SEC. L. & POL'Y 247, 269, 286-87 (2010).

[142] *Id.* at 287 (concluding that government insiders must regard the press as "a more effective agent of change than OIG").

[143] Papandrea, *supra* note 3, at 239 ("Information concerning national security and foreign policy is necessary for citizens to engage in meaningful debate of important public issues. Permitting the government to limit what information the public is given threatens the democratic process.").

[144] *See* Lisa Driscoll, *A Better Way to Handle Whistleblowers: Let Them Speak*, BUS. WK., July 27, 1992, at 36 (postulating that if improper employer behavior is made public, employees will have more confidence in the future that their employers will behave properly).

[145] Goldston et al., *supra* note 14, at 450 ("Had the policymaking apparatus accommodated more criticism in open debate . . . waste and ineptitude could have been discovered, flawed conceptions of national objectives might have been corrected, and policies that better enhanced national security might have been pursued.").

stifles debate on important policy issues both within the government and among the general public.[146]

2. Classification System

Although U.S. law expressly prohibits the disclosure of all classified information, the classified status of a document nonetheless plays an important role in leak prosecutions. It is essential to understand the shortcomings of the classification system in this country to understand why it would be problematic to criminalize the dissemination of classified information wholesale and how the classification system itself contributes to the problem of leaks.

The rapid growth of digital information and the increase in the government's clandestine and covert operations have resulted in an explosion of classified documents. In the "culture of caution" that pervades the intelligence agencies,[147] individuals with classification authority have every incentive to err on the side of classifying information.[148] As more people have access to national security secrets – over 4.9 million people at last count[149] – it is more likely that leaks will occur. But more fundamentally, the excessive classification breeds distrust for the need for secrecy and a lack of respect for the classification stamp.[150]

[146] The Snowden leaks are just the latest demonstration of how little Congress (and the American public) knows about the execution – even the existence – of national security programs that raise fundamental civil liberties concerns. Barton Gellman & Laura Poitras, *U.S. Mines Internet Firms' Data, Documents Show*, WASH. POST, June 7, 2013, at A1; Jillian Rayfield, *Susan Collins: I Wasn't Briefed on PRISM*, SALON (June 11, 2013, 9:12 AM), http://www.salon.com/2013/06/11/susan_collins_i_wasnt_briefed_on_prism, *archived at* http://perma.cc/UH8D-6NM9.

[147] PUB. INTEREST DECLASSIFICATION BD., TRANSFORMING THE SECURITY CLASSIFICATION SYSTEM 3 (2012), *archived at* http://perma.cc/LK8A-4CJJ.

[148] Goitein & Shapiro, *supra* note 44, at 21 ("[T]he incentive structure underlying the current system, in which a multitude of forces pushes in the direction of classification while no force pushes meaningfully in the other direction, virtually ensures that overclassification will occur.").

[149] OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, 2012 REPORT ON SECURITY CLEARANCE DETERMINATIONS 3 (2012), *archived at* http://perma.cc/4HMM-54PK.

[150] *See* SISSELA BOK, SECRETS: ON THE ETHICS OF CONCEALMENT AND REVELATION 217 (1982) ("Leaking has a symbiotic relationship with secrecy."); PRIEST & ARKIN, *supra* note 2; *'Top Secret America': By the Numbers*, WEEK (July 19, 2010), http://theweek.com/article/index/205145/top-secret-america-by-the-numbers, *archived at* http://perma.cc/Y6SN-X54P. The President's Review Group on Intelligence and Communications Technologies recommended that the government "increase transparency and . . . decrease unnecessary secrecy, in order to enhance both accountability and public trust." PRESIDENT'S REVIEW GRP. ON INTELLIGENCE & COMMC'NS TECHS., LIBERTY AND SECURITY IN A CHANGING WORLD 80 (2013), *archived at* http://perma.cc/3SAM-TJZD.

Information is classified based on the assessed level of harm its disclosure would cause to national security.[151] What constitutes the requisite "damage to national security" is unclear; the current executive position simply defines "damage" as "harm," and "national security" as "national defense or foreign relations."[152] Harm can range from tangible to intangible, from concrete to speculative, from imminent to long-term, from minor to severe. As a result, classification is more art than science, often based on subjective rather than objective considerations.[153] Classification determinations are a matter of judgment based on vague criteria and necessarily speculative predictions of harm, and these determinations can be influenced by a variety of bureaucratic concerns and the desire to avoid public controversy.[154]

It is often easiest to identify harms when a disclosure undermines the nation's ability to preserve its physical safety or the safety of its personnel and facilities. Disclosures revealing the movements of troops or ships or the identities of intelligence operatives, sources, and methods typically undermine their effectiveness. But even in these instances, an unauthorized leak can have a positive impact on national security. For example, Jack Goldsmith has observed that the Stuxnet leak may have actually "enhance[d] U.S. cyber deterrence overall" because "it demonstrates that the [United States Government] has sophisticated legal weapons that – despite legal and other obstacles – it is willing to deploy."[155] The same might be said regarding reports that a double agent thwarted another underwear bombing of an airliner.[156] The government claims that now it will make future infiltration difficult, but the leak might also have "sow[ed] some corrosive mistrust among the fanatics."[157] Like these other leaks, Snowden's leaks about widespread NSA surveillance might also make clear to would-be terrorists that the United States will stop at nothing to catch them. In other instances, leaks may hurt national security in the short run but serve to strengthen it in the long run. Defense Secretary Robert Gates has said that he frequently heard about problems he needed to correct only through the media, and not from the affected agencies themselves.

[151] Exec. Order No. 13,526 § 1.2(a)(1)-(3), 75 Fed. Reg. 707, 707-08 (Jan. 5, 2010); Papandrea, *supra* note 3, at 241-42.

[152] Aftergood, *supra* note 134, at 513 (citing Exec. Order No. 13,526, 75 Fed. Reg. at 727, 729).

[153] *See id.*

[154] *See id.* at 519.

[155] Jack Goldsmith, *The Significance of Panetta's Cyber Speech and the Persistent Difficulty of Deterring Cyberattacks*, LAWFARE (Oct. 15, 2012, 1:26 PM), http://www.lawfareblog.com/2012/10/the-significance-of-panettas-cyber-speech-and-the-persistent-difficulty-of-deterring-cyberattacks, *archived at* http://perma.cc/BFW8-8Y3Z.

[156] Scott Shane & Eric Schmitt, *Qaeda Foiled in Plot to Plant Redesigned Bomb on Plane, U.S. Officials Say*, N.Y. TIMES, May 8, 2012, at A12.

[157] Bill Keller, Op-Ed., *The Leak Police*, INT'L HERALD TRIB., Aug. 7, 2012, at 7.

For example, he said that he learned about the lack of armored vehicles in Iraq from a story in *USA Today*.[158]

Some national security harms are intangible and often speculative. Government officials frequently proclaim that the leaker and publisher have placed U.S. soldiers at risk.[159] Government officials also complain that leaks render foreign nations less forthcoming and cooperative with the United States because they cannot trust the United States to keep secrets.[160] In the Bradley Manning sentencing hearings, the judge ruled that the government could present evidence only of harms that resulted directly from his disclosures, and threw out as "speculative" the prosecution's attempts to argue that the leak of U.S. diplomatic cables could dissuade people from seeking help on human rights issues in the future.[161]

Classification decisions are fluid, and they depend upon changing assessments of the risks and benefits of disclosure as well as other more self-serving bureaucratic reasons.[162] In a recent article, Steven Aftergood details the executive branch's shift regarding the necessity of classifying the intelligence budget and the current size of the United States' nuclear weapon stockpile.[163] On these topics, the executive branch went from asserting that secrecy was essential for national security to saying that national security in fact required disclosure.[164] On other matters, the executive decided that declassification served to deflect public criticism. Recently, the executive attempted to deflect

[158] Al Kamen, *Robert Gates on Obama, Leaks and More*, WASH. POST (Mar. 20, 2012, 4:33 PM), http://www.washingtonpost.com/blogs/in-the-loop/post/robert-gates-on-obama-leaks-and-more/2012/03/20/gIQAExr3PS_blog.html, *archived at* http://perma.cc/P6UE-T2F9.

[159] *See, e.g.*, Katie Connolly, *Has Release of WikiLeaks Documents Cost Lives?*, BBC (Dec. 1, 2010), http://www.bbc.co.uk/news/world-us-canada-11882092, *archived at* http://perma.cc/C4UH-VP5J ("US military officials contend that allowing enemies access to their strategic and operational documents creates a dangerous environment for American troops serving abroad."); *James Clapper Says Snowden Damaged US Security*, BBC (Jan. 29, 2014, 4:09 PM), http://www.bbc.co.uk/news/world-us-canada-25954638, *archived at* http://perma.cc/M4CF-9G3D (reporting Clapper's testimony that the Snowden leaks have caused "profound damage" to U.S. national security because "[w]e've lost critical foreign intelligence collection sources," and enemies "are going to school on US intelligence sources, methods and trade craft").

[160] *See* Snepp v. United States, 444 U.S. 507, 512 (1980) (per curiam) ("The continued availability of these [friendly] foreign sources depends upon the CIA's ability to guarantee the security of information that might compromise them and even endanger the personal safety of foreign agents.").

[161] Associated Press, *Bradley Manning Judge Limits Scope of 'Damage' Testimony*, HUFFINGTON POST (Aug. 7, 2013), http://www.huffingtonpost.com/2013/08/07/bradley-manning-testimony_n_3718484.html, *archived at* http://perma.cc/SF4G-AQKT.

[162] *See* Aftergood, *supra* note 134, at 519.

[163] *Id.* at 517-21.

[164] *Id.* at 520.

criticism of NSA's widespread collection of telephone metadata by declassifying information about the program.[165]

Surprisingly, the current classification scheme does not prohibit the classification of information revealing illegal government behavior.[166] Executive orders on classification provide that national security information should not be classified to "conceal violations of law, inefficiency, or administrative error," or "prevent embarrassment to a person, organization, or agency."[167] But these provisions apply only when the classifier had the intent to use the classification system to conceal wrongdoing or embarrassment.[168] In other words, the information is not improperly classified simply because the information pertains to some kind of government wrongdoing or embarrassment.

Another weakness of the classification system is that it does not take into account the public interest in knowing information. To be sure, striking the appropriate balance between an open government and security is extremely difficult. In some instances, the harm is both significant and likely while the public benefit small – like revealing the identities of confidential intelligence sources. In other cases, the risk is small but the public interest great. The hard cases, however, are those where the potential harm to national security interests is great but so too is the benefit to the public interest. The classification system, however, concerns only the first factor – risk to national security – and does not consider the public interest in disclosure, much less whether that interest outweighs the risk to national security.[169] Information regarding major changes in U.S. policy – for example, our policies on torture or surveillance – is typically classified, thereby foreclosing public debate on important issues.[170]

Ideally, Congress would be more aggressive in asserting its power to control the dissemination of national security information. As the Supreme Court has recognized, the executive has unlimited power in this area only if Congress does nothing.[171] Along the same lines, some have suggested that instead of protecting leaks, we should focus on reforming the classification system and methods of challenging overclassification.[172] Disturbingly, some national

---

[165] Press Release, Office of the Dir. of Nat'l Intelligence, Foreign Intelligence Surveillance Court Renews Authority to Collect Telephony Metadata (July 19, 2013), *archived at* http://perma.cc/AD2W-HBRY.

[166] Exec. Order No. 13,526 § 1.7(a)(1)-(2), 75 Fed. Reg. 707, 710 (Jan. 5, 2010).

[167] *Id.*

[168] *See* Stephen L. Vladeck, *Democratic Competence, Constitutional Disorder, and the Freedom of the Press*, 87 WASH. L. REV. 529, 544 (2012).

[169] *See supra* notes 151-54 and accompanying text.

[170] *See* Steven Aftergood, *What Is Overclassification?*, SECRECY NEWS (Oct. 21, 2013), http://blogs.fas.org/secrecy/2013/10/overclass, *archived at* http://perma.cc/6VAG-GQ7M.

[171] *See, e.g.*, Dep't of the Navy v. Egan, 484 U.S. 518, 530 (1988).

[172] Bellia, *supra* note 27, at 1524; Mark Fenster, *Disclosure's Effects: WikiLeaks and*

security agencies have been ignoring important attempts to rein in overclassification. Experts have expressed concern that the secrecy system is increasingly functioning autonomously, outside congressional or executive control.[173] For example, in 2010 the Department of Defense completely ignored a directive from President Obama[174] to issue final implementing regulations for the new executive order on classification policy.[175] National security agencies have also defied orders from Presidents Obama, Bush, and Clinton requiring the automatic declassification of records older than twenty-five years old.[176] As Steven Aftergood has pointed out, the refusal of agencies to release and declassify information despite these directives "casts a different, more positive light on the role of unauthorized disclosures, which in some cases can compensate for the inability or refusal of government agencies to implement binding declassification and disclosure requirements."[177]

Efforts to reform the classification system are ongoing, and they may help curb overclassification. But it is highly unlikely that the classification system will ever do a perfect job of labeling as "secret" only the information that is justifiably confidential. Furthermore, it is essential to recognize that leaks will always play an important role in informing public debate, especially when both Congress and the executive agree to keep essential information from the people.

Recognizing the shortcomings of the classification system is not the same as justifying all leaks. To be sure, in some instances leaks disclose information that should never have been classified; these leaks can play an important role in correcting the rampant and, to date, unsolved overclassification problem. But as commentators have noted, the problem here is whether government insiders should be permitted to evaluate whether the disclosure of certain information would not pose a threat to national security, or that the public value in disclosing such information outweighs any such threat.[178] Neither giving the executive branch exclusive authority to keep secrets nor permitting indiscriminate leaks is a tenable position – a middle ground is needed.

Transparency, 97 IOWA L. REV. 753 (2012).

[173] Steven Aftergood, *Is the Secrecy System an Autonomous Entity?*, SECRECY NEWS (Mar. 21, 2011), http://www.fas.org/blog/secrecy/2011/03/autonomous.html, *archived at* http://perma.cc/N3CL-TZBF.

[174] Memorandum on Implementation of the Executive Order, "Classified National Security Information," 2009 DAILY COMP. PRES. DOC. 1023 (Dec. 29, 2009).

[175] Steven Aftergood, *Secrecy Reform Stymied by Pentagon*, SECRECY NEWS (Feb. 24, 2011), http://www.fas.org/blog/secrecy/2011/02/reform_stymied.html, *archived at* http://perma.cc/ZZ2F-A6Y6.

[176] Aftergood, *supra* note 173.

[177] *Id.*

[178] *See* Bellia, *supra* note 27, at 1505.

3. Concerns About Leaks

Our country has a complicated relationship with leakers. This is not surprising given that there are many different types of leaks, from a variety of sources, to a variety of recipients (especially in the digital age), for a variety of different motives. The value and harm of the information revealed – to the extent value and harm can even be calculated – add more variability to the relationship. In a time of war or national crisis, concerns about interfering with the executive's expertise on national security information are heightened.

One reason for the unease about leaks is that there are so many different kinds. At one end of the spectrum is the intentional leak to the enemy made with the purpose to help the enemy or harm the United States. At the other end is the selfless, morally compelled government insider who wants to expose government wrongdoing to the American public no matter what the personal cost. Most leaks fall somewhere in between these two poles.

Although the leak prosecutions the government has undertaken all involve lower-level employees, by all accounts the "game of leaks" is most frequently one played by high-level officials.[179] Some government officials leak in order to promote the Administration's agenda,[180] or to undermine the Administration's foes,[181] or to float a "trial balloon" to gauge public reaction to a proposed initiative.[182] Sometimes a leak might more accurately be described as a plant made by political operatives as an effort to "manage the news, and orchestrate public debate from behind the scenes."[183] Government officials also use leaks to influence another branch of government or to reach a foreign country (often with "disinformation").[184] One significant concern those opposed to the recent leak prosecutions raise is that the government does not tend to prosecute the leaks that it likes.[185] For example, the government has

[179] Levi, *supra* note 15, at 624.

[180] *Id.* at 628-29.

[181] *See Former CIA Officer Claims Conspiracy Outed Her Identity*, CNN (July 14, 2006), http://www.cnn.com/2006/POLITICS/07/14/cialeak.lawsuit/index.html, *archived at* http://perma.cc/TP2H-68KP (quoting Valerie Plame, who claimed that the leak of her CIA affiliation "was motivated by an invidiously discriminatory animus toward those who had publicly criticized the administration's stated justifications for going to war").

[182] Papandrea, *supra* note 3, at 250; Pozen, *supra* note 26, at 559.

[183] Levi, *supra* note 15, at 611; *see also* STAFF OF SUBCOMM. ON CIVIL & CONSTITUTIONAL RIGHTS OF THE H. COMM. ON THE JUDICIARY, 98TH CONG., REP. OF THE INTERDEPARTMENTAL GROUP ON UNAUTHORIZED DISCLOSURES OF CLASSIFIED INFO. 1 (Comm. Print 1985) ("It should be noted that some high ranking officials believe they have the authority to leak classified information in furtherance of government policy."); Levi, *supra* note 15, 628-29. For a more complete discussion of the different types of leaks, see Levi, *supra* note 15, at 623-31; Papandrea, *supra* note 3, at 248-57; Pozen, *supra* note 26.

[184] Papandrea, *supra* note 3, at 252-53.

[185] Glenn Greenwald, *Why Are Bob Woodward's WH Sources – or Woodward Himself – Not on Trial Next to Bradley Manning?*, GUARDIAN (Jan. 10, 2013, 8:02 AM), http://www.theguardian.com/commentisfree/2013/jan/10/manning-prosecution-press-freedom-woodwar

made no indication it plans on prosecuting Bob Woodward's sources, who revealed some of the nation's most sensitive secrets.

The most common argument against protecting leakers is, of course, that their disclosures harm the country's national security. Although the government has not done a particularly good job of explaining exactly how any particular leak has directly harmed national security, it does seem likely that some leaks cause harm. As discussed above, harms may be intangible, speculative, and hard to quantify. Some critics have argued that the difficulty of determining harm is precisely the reason why government insiders should not be able to deputize themselves to decide when the disclosure of information would be the best thing for the American people.[186] Information that may seem innocuous to a lower-level employee may in fact have the potential to cause great harm if revealed.[187] As President Obama has argued: "If any individual who objects to government policy can take it into their own hands to publicly disclose classified information, then we will not be able to keep our people safe, or conduct foreign policy."[188]

In some instances, it is also difficult to determine when a leak adds value to the public debate.[189] Some commentators contend that WikiLeaks' disclosure of thousands of documents about the war in Afghanistan and 250,000 American diplomatic cables has helped Americans become "exponentially more informed about the many facets of American involvement in Afghanistan and about the numerous issues of American foreign policy reflected in the once-secret cables."[190] Others contend just as vigorously that these disclosures cause far more harm than good and contribute little to the public discussion.[191] Some leaks can undermine public debate if they are inaccurate or tell only part of the story. Even reporter Declan Walsh, who has called leaks "the unfiltered lifeblood of investigative journalism," concedes that leaks "may come from difficult, even compromised sources, be ridden with impurities and require

d, *archived at* http://perma.cc/YA6W-55UL (decrying the fact that the government is prosecuting Manning, but not Woodward, for leaks).

[186] *See, e.g.*, 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, 399 (1986) (claiming such power would be "preposterous"); *The Supreme Court, 1970 Term*, 85 HARV. L. REV. 38, 211 (1971) (arguing that it is not the role of a federal employee to balance the public's right to know against the harm disclosure would cause).

[187] Edgar & Schmidt, Jr., *supra* note 186, at 400.

[188] Jane Meyer, *Snowden Calls Russian-Spy Story "Absurd" in Exclusive Interview*, NEW YORKER (Jan. 21, 2014), http://www.newyorker.com/online/blogs/newsdesk/2014/01/snowden-calls-russian-spy-story-absurd.html, *archived at* http://perma.cc/C9DP-JSJB.

[189] Fenster, *supra* note 172, at 799.

[190] Robert A. Sedler, *Self-Censorship and the First Amendment*, 25 NOTRE DAME J.L. ETHICS & PUB. POL'Y 13, 42 (2011).

[191] See Fenster, *supra* note 172, for a more extensive discussion regarding the difficulties of determining the value of the Bradley Manning disclosures.

careful handling to produce an accurate story."[192] "Plants" that selectively disclose classified information are particularly likely to skew the public's understanding, but so might leaks from lower-level employees. For President Obama, the Snowden leaks are a perfect example of this because they present a misleading portrait of the government's surveillance activities.[193] In order to counteract the alleged misinformation or misperceptions the leak caused, the government felt forced to reveal even more information about programs they would have preferred to keep secret.[194]

On the other hand, some leaks clearly do contribute significantly to public debate. For example, even government officials have conceded that the Snowden leaks have generated substantial public debate. In an order releasing Foreign Intelligence Surveillance Court (FISC) opinions regarding NSA surveillance revealed by Snowden's leaks, FISC Judge Dennis Saylor IV explained that Snowden's leaks, as well as the government's statements in response, "have engaged considerable public interest and debate about Section 215."[195] This public debate raises the question of whether NSA's massive surveillance activities should have ever been classified in the first place.

Another related concern is that some leaks undermine the democratic process. Many scholars who recognize the rampant overclassification of information and the important role leaks have played in informing public debate about important issues express concern about giving a "disgruntled employee" the ability to disrupt government programs and policies.[196] With respect to the Snowden leaks, President Obama claimed (perhaps disingenuously) that the timing of Snowden's disclosures short circuited a more orderly and "thoughtful fact-based debate" about the challenged surveillance operations.[197]

---

[192] Sullivan, *supra* note 68, at SR12.

[193] *See* Meyer, *supra* note 188 (explaining that President Obama said that the media reporting of the Snowden leaks "has often shed more heat than light").

[194] Press Release, Office of the Dir. of Nat'l Intelligence, DNI Clapper Declassifies Additional Intelligence Community Documents Regarding Collection Under Section 501 of the Foreign Intelligence Surveillance Act (Nov. 18, 2013), *archived at* http://perma.cc/K8DU-Q87H.

[195] *In re* Orders of this Court Interpreting Sec. 215 of the Patriot Act, No. MISC. 13-02, 2013 WL 5460064, at *7 (Foreign Intelligence Surveillance Ct. Sept. 13, 2013).

[196] *See, e.g.*, Bellia, *supra* note 27, at 1505 ("[A] regime for national security information . . . must also account for the malicious, disgruntled, or misguided insider who seeks to override judgments about national security and harm made within the framework established by Congress and the executive."); Eugene Volokh, *Leakers, Recipients, and Conspirators*, VOLOKH CONSPIRACY (May 21, 2013, 12:04 PM), http://www.volokh.com/2013/05/21/leakers-recipients-and-conspirators, *archived at* http://perma.cc/J72U-8Z4R.

[197] Z. Byron Wolf, *Fact-Checking Obama's Claims About Snowden*, CNN (Aug. 13, 2013), http://www.cnn.com/2013/08/12/politics/obama-snowden-whistleblower, *archived at* http://perma.cc/WGJ7-N3KH.

Some commentators fear that if government insiders were entitled to reveal sensitive information, government officials would likely curtail information sharing in largely negative ways. Thus, fearful of leaks, government officials would share sensitive information with only a small circle of trusted employees, undermining the thoughtfulness of the decisionmaking process and, ultimately, our security efforts.[198] Judicially sanctioned leaking also may undermine cooperative efforts between government agencies and with foreign entities (which logically would be less likely to share sensitive information).[199] In light of Bradley Manning's disclosures, the government should be more careful about who has access to information. Obviously, allowing government insiders to reveal classified information willy nilly is bound to reduce the quality of government decisionmaking.

4. The Name Game

The uncertainty regarding leakers has led to a vigorous "name game" as commentators, public officials and lawyers argue whether someone is a traitor, spy, or whistleblower.[200] The lines between each category have always been blurry, but changes in technology have made them more difficult to discern than ever.

From the government's point of view, the various labels for leakers are irrelevant because the potential harm of the disclosures is the same whether the information is delivered directly to Al Qaeda or published in the *New York*

[198] Edgar & Schmidt, Jr., *supra* note 186, at 399-400 ("Any such privilege [for government employees to decide to reveal secrets], if regularly exercised, will lead inevitably to a concentration of power in the hands of those few people whose unquestioned personal loyalty to their superiors makes them a safe security risk."); Katz, *supra* note 6, at 111 (discussing the threat to "an open decision-making process" posed by leaks).

[199] Katz, *supra* note 6, at 112.

[200] *See, e.g.*, Caitlin Emma, *Hayden Labels Snowden a 'Defector,'* POLITICO (Aug. 11, 2013, 10:54 AM), http://www.politico.com/blogs/politico-live/2013/08/hayden-snowden-a-defector-170345.html, *archived at* http://perma.cc/XW7T-4NZG; Tal Kopan, *Poll: Edward Snowden Still a 'Whistleblower,'* POLITICO (Aug. 1, 2013, 10:52 AM), http://www.politico.com/story/2013/08/edward-snowden-nsa-leak-poll-95054.html, *archived at* http://perma.cc/HQ4U-ZV46 (explaining that fifty-five percent of those polled said Snowden was a whistleblower, while thirty-four percent called him a traitor); Tom McCarthy, *Richard Cohen's Reverse on Snowden: Not a "Traitor," But a Whistleblower*, GUARDIAN (Oct. 22, 2013), http://www.theguardian.com/commentisfree/2013/oct/22/richard-cohen-reverse-edward-snowden, *archived at* http://perma.cc/MC29-7JE9 (reporting that *Washington Post* columnist Richard Cohen first labeled Snowden a "traitor" but later concluded Snowden "lacks the requisite intent and menace" to qualify as such); Meyer, *supra* note 188 (reporting that Senator Diane Feinstein "did not dismiss the notion" that Snowden "may have had help from the Russians"); Maya Rhodan, *Dick Cheney Calls Snowden a "Traitor," Defends NSA*, TIME (Oct. 28, 2013), http://swampland.time.com/2013/10/28/dick-cheney-calls-snowden-a-traitor-defends-nsa, *archived at* http://perma.cc/JY2E-SWNW.

Times: our enemies obtain access to our secrets.[201] In the national dialogue, however, these labels are relevant to the determination of who deserves praise and who should be condemned. The debate tends to focus on what was revealed, to whom it was revealed, and why it was revealed.

Although defenders of leakers like Snowden and Manning would rather see them labeled "whistleblowers" than "traitors" or "spies," whistleblowers are not universally beloved.[202] In the United States, individuals who reveal wrongdoing are subject to a variety of negative epithets, including "disgruntled or disruptive employee," "informer," and "snitch, grass, rat, rat fink, stoolie, stool pigeon, squealer, tattletale, backstabber, skunk, spy, mole, and traitor."[203] Some organizations fear that whistleblowers threaten "a loss of group identity, loyalty, and morale, and a consequent loss of efficiency."[204] A government official who deals with whistleblowers reflected these concerns when he said that "[i]f we didn't have loyalty, nothing would get done in this government."[205]

Although historically whistleblowers may have been distrusted, in the last several decades whistleblower protections have become part of the "cultural

[201] Indeed, from the government's point of view, disclosures to the press potentially cause greater harm because such information reaches "all our enemies," not just one. *See* Hon. George Ellard, Inspector General, NSA, Remarks at the Georgetown Journal of National Security Law and Policy Symposium: Leakers, Whistleblowers and Traitors: An Evolving Paradigm, at 03:48:00 (Feb. 25, 2014), *available at* http://apps.law.georgetown.edu/webcasts/eventDetail.cfm?eventID=2275 (arguing that the Snowden leaks caused more damage than those of convicted spy Robert Hanssen, who sold secrets to the Russian and Soviet intelligence services).

[202] Orly Lobel, *Linking Prevention, Detection, and Whistleblowing: Principles for Designing Effective Reporting Systems*, 54 S. TEX. L. REV. 37, 40 (2012) (explaining that the United States has an "uneasy" image of whistleblowers, "rang[ing] from hero to snitch; from saint to traitor"). Those who suffered adverse consequences as a result of whistleblowing are less likely to regard a whistleblower charitably. *See, e.g.*, Dawn Bryant, *Abu Ghraib Whistleblower's Ordeal*, BBC (Aug. 5, 2007, 5:02 AM), http://news.bbc.co.uk/2/hi/6930197.stm, *archived at* http://perma.cc/BFQ7-CTFP (remarking that some members of the military regard Joe Darby, who disclosed pictures of prisoner abuse at Abu Ghraib, as a traitor).

[203] ROBERT G. VAUGHN, THE SUCCESSES AND FAILURES OF WHISTLEBLOWER LAWS 255 (2012). Vaughn points out that in some languages, there appears to be no positive words at all for those who make unauthorized disclosures. *Id.* Curiously, Vaughn observes, British law uses the term "public interest disclosure" and not "whistleblower," and the United Nations Convention Against Corruption uses the term "reporting persons" because "whistleblower" is "a colloquialism that cannot be accurately and precisely translated into many languages." *Id.* at 257.

[204] Elletta Sangrey Callahan & Terry Morehead Dworkin, *Do Good and Get Rich: Financial Incentives for Whistleblowing and the False Claims Act*, 37 VILL. L. REV. 273, 333 (1992).

[205] FRED ALFORD, WHISTLEBLOWERS: BROKEN LIVES AND ORGANIZATIONAL POWER 9 (2001).

landscape" in the United States.[206] Professor Robert Vaughn has offered a compelling narrative about how the civil rights movement influenced the acceptance of whistleblowing. Notably, Vaughn points out, a "clear theme in most whistleblower narratives" is that "whistleblowers voluntarily proceed in the face of personal suffering in order to disclose misconduct and to pursue their allegations."[207] The passage of federal whistleblower laws arose out of a "perfect storm" of events in the late 1960s and 70s, including "the positive narratives of whistleblowers, the changing perceptions of the place of the individual in large institutions, and the discontent and dissent generated by the civil rights and antiwar movements."[208] These developments led to popular concerns about "the risk of government institutions run by 'team players' and 'yea sayers.'"[209]

For some, whistleblowing remains a form of civil disobedience that should not receive any legal protection.[210] Those challenging Snowden's classification as a whistleblower point to his failure to stay in the United States and accept whatever punishment might result from his unauthorized disclosure of national security information. For example, former Secretary of Defense Robert Gates has argued that, if Snowden were truly motivated to reveal wrongdoing, "he should come home and face the music, much as earlier whistleblowers like Daniel Ellsberg and others did."[211] Other critics have made similar arguments, on both sides of the political spectrum.[212]

---

[206] VAUGHN, *supra* note 203, at 257. Vaughn speculates that support for whistleblowers in the United States may stem in part from the country's strong commitment to individualism and personal fulfillment. *Id.* at 257-58.

[207] ALFORD, *supra* note 205, at 45; *see also id.* at 33-46 (discussing how the civil rights movement influenced the public acceptance of whistleblowing).

[208] *Id.* at 89.

[209] *Id.*

[210] Brian Dalton, *Whistleblowers and Treasonous Heroes*, ABOVE L. (Sept. 24, 2013, 4:32 PM), http://abovethelaw.com/2013/09/whistleblowers-and-treasonous-heroes, *archived at* http://perma.cc/9Z69-XBLZ ("Whistleblowing as an act of civil disobedience is an acknowledgement that the law will not offer any protection."); Gabriel Schoenfeld, *How to Be an Honest Whistleblower*, WALL ST. J., June 10, 2011, at A13 ("[C]ivil disobedience in a democracy entails accepting the consequences of defying the law in defense of one's convictions."). John Rawls has similarly argued that civil disobedience "is done in a situation where arrest and punishment are expected and accepted without resistance." JOHN RAWLS, *The Justification of Civil Disobedience*, *in* COLLECTED PAPERS: JOHN RAWLS 182 (Samuel Freeman ed., 1999).

[211] *PBS Newshour* (PBS television broadcast Jan. 14, 2014).

[212] *See, e.g.*, Thomas Friedman, Op-Ed., *Obama, Snowden and Putin*, N.Y. TIMES, Aug. 14, 2013, at A23 (arguing that if Snowden wants to "make a second impression – that he truly is a whistle-blower, not a traitor," he "need[s] to come home, make his case and face his accusers"); *State of the Union with Candy Crowley: Interview with Sen. Chuck Schumer* (CNN television broadcast June 23, 2013) (transcript archived at http://perma.cc/FW9M-XVSN) (arguing Snowden is not a "great human rights crusader" because he fled the country,

Many state and federal statutes enacted precisely to encourage whistleblowing, however, take a different view.[213] The trick to determining the appropriate scope of whistleblowing protections is to determine which disclosures constitute the ethical and moral behavior we as a society wish to encourage and protect.[214]

Whistleblower protections are based primarily upon what information the insider reveals. Generally, state and federal whistleblower statutes protect reports of illegality, fraud, waste, corruption, or abuse. Many statutes do not require the disclosures to be correct as long the insider reasonably believes wrongdoing has occurred.[215] Protecting good faith allegations of wrongdoing is particularly important in the national security arena. It is often difficult, if not impossible, to determine whether particular government conduct or action is unconstitutional or otherwise unlawful,[216] and "presidents can – and do – cite the public interest as the justification for any violation of the law."[217]

In the public debate, a leaker's motive plays a large role in the popular conception of who is deserving of praise,[218] and may play a role in the Court's treatment of a particular defendant.[219] For example, when Samuel Morison was prosecuted for leaking satellite photos to *Jane's Defence Weekly*, a British magazine, the government argued that he leaked the photos in order to better his chances of receiving a permanent position with the publication.[220] This self-serving motivation may have played a role in the Court's unwillingness to recognize his First Amendment defense.[221] The narrative surrounding the

unlike Daniel Ellsberg and other famous civil disobedients who "faced the consequences").

[213] *See State Whistleblower Laws*, NAT'L CONFERENCE OF STATE LEGISLATURES (Nov. 2010), http://www.ncsl.org/research/labor-and-employment/state-whistleblower-laws.aspx, *archived at* http://perma.cc/CF9A-G7FS.

[214] *See, e.g.*, Nicholas M. Rongine, *Toward a Coherent Legal Response to the Public Policy Dilemma Posed by Whistleblowing*, 23 AM. BUS. L.J. 281, 282 (1985).

[215] *See, e.g.*, *infra* notes 253-60.

[216] Blasi, *supra* note 13, at 543.

[217] SAGAR, *supra* note 85, at 138.

[218] Steven Aftergood, *"Traitor," A Whistleblower's Tale*, SECRECY NEWS (Apr. 16, 2012), http://blogs.fas.org/secrecy/2012/04/traitor, *archived at* http://perma.cc/MT7E-53B4 (stating that the term "whistleblower" "presumes the pure intention of the individual challenger").

[219] Motive also plays a role in the government's decisions about which leaks to prosecute. *See* Kenneth Wainstein, Remarks at the Georgetown Journal of National Security Law and Policy Symposium: Leakers, Whistleblowers and Traitors: An Evolving Paradigm, at 04:14:00 (Feb. 25, 2014), *available at* http://apps.law.georgetown.edu/webcasts/eventDetail.cfm?eventID=2275. Wainstein made clear, however, that salutary motives do not give people a "pass" because otherwise "there goes your classification system." *Id.*

[220] Lincoln Caplin, *Leaks and Consequences*, AM. SCHOLAR (Autumn 2013), http://theamericanscholar.org/leaks-and-consequences/#.UnbTzpG5kds, *archived at* http://perma.cc/J59L-AFEL.

[221] *Id.* Morison claimed that he disclosed the photographs because he felt that publicizing

Manning and Snowden leaks has also focused on the motivations for their leaks. [222] Manning is portrayed as a troubled young man who leaked in a desperate plea for attention;[223] Snowden was initially characterized as a "high school dropout" with a "Mother Teresa gene."[224] Yet both of them claim they made their disclosures to reveal the government's wrongdoing to the American public.[225] Even someone who reveals plainly unlawful government conduct might have a more selfish motive and leak information "for spiteful or petty reasons . . . [or in order to] insulate [themselves] from disciplinary or other personnel actions."[226] In any given case, a leaker might have multiple motivations, some praiseworthy and some less so.

Although it can be difficult to determine the reason why someone reveals information, some states incorporate questions of motive into their definition of what constitutes protected whistleblowing, and courts frequently consider motive regardless of whether they are statutorily required to do so.[227] Many states are reluctant to protect individuals who stand to gain from their disclosures. For example, Wisconsin law denies protection to any whistleblower whose disclosures are motivated by gaining "anything of value" – unless it is a reward offered by the state.[228] Both Pennsylvania's and West Virginia's laws only protect good-faith reports of wrongdoing that are "made without malice or consideration of personal benefit."[229] Congress is more

the progress of the Soviets would enable the Navy to obtain greater appropriations. *Id.*

[222] *See* Glenn Greenwald et al., *Edward Snowden: The Whistleblower Behind the NSA Surveillance Revelations*, GUARDIAN (June 9, 2013), http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance?guni=Podcast:in%20body%20link, *archived at* http://perma.cc/9EJT-VFUB; Glenn Greenwald, *The Motives of Bradley Manning*, SALON (July 4, 2011, 8:05 AM), http://www.salon.com/2011/07/04/manning_11, *archived at* http://perma.cc/PL7C-ES2E.

[223] Associated Press, *Bradley Manning Wanted Attention for Spilling to WikiLeaks, Prosecutors Say*, CBS NEWS (July 25, 2013, 3:31 PM), http://www.cbsnews.com/news/bradley-manning-wanted-attention-for-spilling-to-wikileaks-prosecutors-say, *archived at* http://perma.cc/3LZT-QPVQ.

[224] Barbara Starr & Holly Yan, *Man Behind NSA Leaks Says He Did It to Safeguard Privacy, Liberty*, CNN (June 23, 2013), http://www.cnn.com/2013/06/10/politics/edward-snowden-profile, *archived at* http://perma.cc/Y6VV-RVUQ.

[225] Greenwald et al., *supra* note 222; Starr & Yan, *supra* note 224.

[226] Robert Vaughn, *Statutory Protection of Whistleblowers in the Federal Executive Branch*, 1982 U. ILL. L. REV. 615, 617.

[227] *See, e.g.*, Forsyth v. City of Dall., 91 F.3d 769, 773 (5th Cir. 1996) (stating that police officers who had revealed allegedly illegal wiretapping were primarily motivated by public, and not personal, concerns).

[228] WIS. STAT. ANN. § 230.83(2) (West 2009) ("This section does not apply to an employee who discloses information if the employee knows or anticipates that the disclosure is likely to result in the receipt of anything of value . . . unless the employee discloses information in pursuit of any award offered by any governmental unit . . . .").

[229] 43 PA. CONS. STAT. ANN. § 1422 (West 1986); *see also* W. VA. CODE ANN. § 6C-1-

willing to offer monetary awards to whistleblowers to encourage them to come forward.[230]

Although motive plays a significant role in the popular debate about which unauthorized disclosures are worthy of protection, most legal scholars and social scientists have tended to agree that motive is irrelevant when disclosures reveal clear wrongdoing.[231] In such instances, what is important is whether the "whistleblowing provides information beneficial to societal interests."[232] Motive potentially plays a more important role when it turns out that the disclosure does not, in fact, reveal wrongdoing because it can serve "as a reflection of the whistleblower's good faith belief in the legitimacy of the information about the wrongdoing."[233]

One big issue regarding the definition of whistleblower is whether those who reveal information to the press can ever be included in that category. Most whistleblower statutes do not protect disclosures that are not made through the official channels.[234] The lack of protection for public disclosures is most likely based on the belief that whistleblowers who truly care about correcting wrongdoing – as opposed to self-aggrandizing or publicity – are more likely to report misconduct internally within the government agency than to a reporter.[235] This assumption may prove incorrect in some cases; an employee may disclose information to the media because the internal agency is too corrupt to handle it appropriately, or because internal efforts to remedy the problem were ignored. A whistleblower may also choose to go to the media to avoid retaliation, even though such a route does not guarantee a whistleblower's anonymity.[236] Whistleblowing to the media is particularly appropriate when internal avenues have not responded adequately or the

2(g) (LexisNexis 2010).

[230] *See, e.g.*, Insider Trading and Securities Fraud Enforcement Act of 1988, 15 U.S.C. § 78u-1(e) (supplying authority to award monetary rewards to informants); False Claims Act, 31 U.S.C. § 3730 (2012). For an interesting analysis of the psychological effectiveness of monetary rewards, see Callahan & Dworkin, *supra* note 204, at 273.

[231] Callahan & Dworkin, *supra* note 204, at 319-20.

[232] *Id.*

[233] *Id.*; *see also* SAGAR, *supra* note 85, at 137 (arguing that, while motive is not important when insiders reveal "gross or obvious wrongdoing," motive matters when the disclosures involve "suspected or prima facie wrongdoing").

[234] Terry Morehead Dworkin & Elletta Sangrey Callahan, *Employee Disclosures to the Media: When Is a "Source" a "Sourcerer"?*, 15 HASTINGS COMM. & ENT. L.J. 357, 368-69 (1993).

[235] *Id.* at 369. They may also be based on the hope that the agency can correct wrongdoing on its own. *Id.* at 378.

[236] Although over thirty states and the District of Columbia recognize some form of the reporters' privilege, in many states the privilege is not absolute. Mary-Rose Papandrea, *Citizen Journalism and the Reporter's Privilege*, 91 MINN. L. REV. 515, 545-46 (2007). In addition, efforts to pass a federal statutory shield law have not yet been successful, and the availability of a constitutional or common law privilege is not certain. *Id.* at 564.

employee suffers retaliation.[237] Thus, although the federal whistleblowing statutes do not protect disclosures made directly to public, some commentators will sometimes label such disclosures "whistleblowing" whenever they reveal illegal behavior, waste, fraud, mismanagement, or other questionable conduct.

Espionage is distinct from disclosures to the press in crucial ways. Espionage is a form of information gathering, but it is conducted in a clandestine manner, so that the fact that the information has been communicated, as well as the information itself, is kept secret.[238] Inherent in the definition of espionage is some sort of relationship or agreement between the spy and another country or foreign power. Because the recipient of covertly shared information knows who the source of that information is, the information is more trustworthy and credible than information published in the media based on disclosures from anonymous sources. Most importantly, in the case of traditional espionage, the United States does not know which of its secrets have been compromised and accordingly cannot take steps to limit the damage.[239]

Those engaged in espionage do not always give secrets to our enemies; sometimes they give them to our friends. Take, for example, the spy Jonathan Pollard, who sold U.S. intelligence secrets to Israel.[240] One reason that selling secrets to our allies is criminalized is that allies do not always agree with each other's policies, and they are not willing to exchange all of their intelligence information.[241]

---

[237] Dworkin & Callahan, *supra* note 234, at 397 ("With reference to public employee whistleblowers, information about organizational misconduct may be conveyed legitimately to the media in instances where intragovernmental authorities have failed to respond, have not responded in an adequate manner, or where the whistleblower has experienced retaliation for reporting.").

[238] The British Security Service defines espionage as "a process which involves human sources (agents) or technical means to obtain information which is not normally publically available. It may also involve seeking to influence decision makers and opinion-formers to benefit a foreign power." *What Is Espionage?*, SEC. SERVICE: MI5, https://www.mi5.gov.uk/home/the-threats/espionage/what-is-espionage.html (last visited Jan. 10, 2014), *archived at* http://perma.cc/ZL64-ESNE.

[239] Edgar & Schmidt, Jr., *supra* note 186, at 400-01 (arguing that "the greatest damage" to national security occurs in cases of traditional espionage because the government mistakenly believes that its "secrets are secret" (internal quotation marks omitted)). In addition, foreign governments may be less willing to trust the information in the media because they do not know the media's anonymous sources in the same way they know their own agents. *See id.* at 401.

[240] *Kerry Reportedly Says He Will Consider Freeing Jonathan Pollard as Part of Prisoner Swap*, FOX NEWS (Dec. 29, 2013), http://www.foxnews.com/politics/2013/12/29/kerry-returns-to-israel-to-talk-with-leaders-about-peace-negotiations-amid-new, *archived at* http://perma.cc/7ZL8-8MY7.

[241] *See* Bernard Weintraub, *The Darker Side of U.S.-Israeli Ties Revealed*, N.Y. TIMES, June 5, 1986, at B9. One commentator explained that Israel was "frustrated by the refusal of the United States to provide certain information on troop deployments by moderate Arab

Motivation is not particularly helpful in defining espionage. People have had various motivations for committing espionage: (1) desire for money or other financial rewards; (2) ideological affinity[242] (communism, fundamental Islamic causes, etc.); (3) a desire to avoid embarrassment; (4) sexual gratification; (5) enjoyment of the "thrill" of spying; and (6) the need to feel important, redress perceived lack of appreciation, or unfair treatment, or a feeling of frustration. Individuals who seek out spying opportunities are most likely to be motivated by personal reasons, including frustration at work and delusions of grandeur.[243] Examples include Edward Lee Howard, who defected to the Soviet Union after the CIA fired him; Aldrich Ames, whose government career had stalled; Robert Hanssen, who believed that his colleagues at the FBI did not appreciate him as much as they should; and Earl Edwin Pitts, who sought revenge against his FBI superiors.[244] One important trend since the end of the Cold War is that the majority of spies who have disclosed information to foreign powers are naturalized citizens who have a pre-existing connection to another country.[245] Many of these spies are not compensated; money is not their motivation.[246] They may feel loyalty to their native land and feel alienated in the United States.[247]

A potentially more helpful factor in distinguishing among traitors, spies, and other leakers is *to whom* the disclosures are made, but even this factor has potential difficulties. When we think of spies we might think of secret meetings in a dark place where classified documents are exchanged for money.

countries, including Jordan and Egypt. Moreover, some Israelis have said that the United States declined to turn over all the intelligence data that would be helpful in protecting Israel." *Id.*

[242] Julius and Ethel Rosenberg are examples of spies with a strong ideological motivation; they strongly supported the communist movement in the Soviet Union. Sam Roberts, Book Review, *The Rosenbergs Revisited*, N.Y. TIMES, Oct. 10, 2010, at BR23.

[243] Erin Creegan, *National Security Crime*, 3 HARV. NAT'L SEC. J. 373, 409-10 (2012) ("Alienated spies are those who betray their country for personal reasons. The most common reasons seem to be: a perception of unfair treatment in their government jobs, a sense of personal importance and frustration when others fail to acknowledge these delusions of grandeur, a need to be important . . . .").

[244] *Id.* at 409-10.

[245] *Id.* at 413 ("This report claims that most spies since 1990 have spied out of loyalty to another country, with money as a motivation coming second and disgruntlement, noted above, a third-place motivator.").

[246] *Id.*

[247] *Id.* Terrorists like the Boston Marathon bombers also may fit this profile. Akbar Ahmed, *Opinion: Boston Bombings Show Muslims Between Worlds*, NAT'L GEOGRAPHIC NEWS (Apr. 22, 2013), http://news.nationalgeographic.com/news/2013/13/130422-boston-marathon-bombings-terrorism-islam-muslims-chechnya-opinion, *archived at* http://perma.cc/BP3B-75ZV ("[T]he suspected bombers found themselves suspended in that dangerous territory between two worlds—the old not quite faded from their lives and the new still too new to absorb them.").

Certainly any direct delivery of information to a foreign nation or its agents tends to be a sign of espionage, if not treason. But espionage and treason can be committed through a more indirect method of delivery. The government attorneys prosecuting Bradley Manning have pointed to Civil War cases in which individuals were convicted of aiding and abetting the enemy based on the inclusion of information in a widely circulated publication.[248] In one case, a Union officer was convicted after he gave a Virginia newspaper a list of the rosters of Union units.[249] The precise facts of this case are unclear – Manning contends that in these Civil War cases the publications contained coded messages – but at the very least they demonstrate that sometimes the exchange of information with the enemy can be indirect.[250] Thus, it might be important to focus not solely on "to whom" disclosures are made, but rather on to whom the leaker intended the audience for his disclosures to be.

II. PROTECTIONS AND PENALTIES

Anyone who discloses national security information without authorization potentially faces a broad range of civil and criminal sanctions. The current statutory scheme does not do a particularly good job of distinguishing among traitors, spies, whistleblowers in the intelligence community, and every other leaker. The statutory protections for whistleblowers are woefully insufficient and, given the current political atmosphere, unlikely to improve any time soon. Indeed, the Obama Administration has been largely supportive of whistleblowers generally, but has strongly resisted extending the same robust protections to government insiders with access to national security information.[251] A recent presidential policy directive provides national security employees with some additional whistleblowing protections they have not enjoyed until now, but these protections still fall far short of what other government employees have, and they do not cover government contractors.[252] In addition, national security whistleblowers have little shelter from retaliation, and the judicial branch has no authority to review any retaliation claims they might have.[253] As a result, the executive branch has virtually unchecked authority to declare what information is secret and to punish leakers as it sees fit.[254]

---

[248] Yochai Benkler, *The Dangerous Logic of the Bradley Manning Case*, NEW REPUBLIC (Mar. 1, 2013), http://www.newrepublic.com/article/112554, *archived at* http://perma.cc/P993-8JAF.

[249] *Id.*

[250] *Id.*

[251] Moberly, *supra* note 67, at 95.

[252] Presidential Policy Directive/PPD-19: Protecting Whistleblowers with Access to Classified Information (Oct. 10, 2012), *archived at* http://perma.cc/NQ2T-WYHA.

[253] *See, e.g.*, Intelligence Community Whistleblower Protection Act of 1998, Pub. L. No. 105-272, §§ 702-703, 112 Stat. 2396, 2414-17 (specifically prohibiting judicial review).

[254] Edgar & Schmidt, Jr., *supra* note 186, at 356.

A. *Statutory and Regulatory Protections*

The government often claims that it is unnecessary to search, actively prevent, or protect against national security leakers because there are adequate official channels through which whistleblowers may expose wrongdoing.[255] This is not the case. As Stephen Vladeck has observed, the current legal regime "would give pause to even the most altruistic and well-intentioned whistleblowers."[256]

The paucity of protections for national security employees stands in great contrast to the safeguards afforded to other government employees. The Federal Whistleblower Protection Act (WPA) protects a government employee who discloses information that he "reasonably believes" demonstrates a violation of any law, rule, or regulation, an instance of gross mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety, so long as he is not prohibited by law or required by executive order to keep the information secret.[257] Other federal laws in certain situations protect whistleblowers who act on a "reasonable belief" of wrongdoing[258]; still others protect those who report "potential"[259] or "alleged"[260] violations of federal law.[261] The reason for protecting these good faith beliefs is to encourage disclosures.[262]

The WPA offers virtually no protection to national security employees and contractors.[263] First, the WPA makes no mention of contractors at all and

[255] *See, e.g.*, Larissa Epatko, *Former Defense Secretary Gates Calls NSA Leaker Snowden a 'Traitor,'* PBS (Jan. 14, 2014, 12:11 PM), http://www.pbs.org/newshour/rundown/gates-on-snowden, *archived at* http://perma.cc/7FFQ-ACPF (recounting Secretary Gates' comments that there are "avenues" within the intelligence community to report government wrongdoing, and that Snowden's decision to go to the media instead is "an extraordinary act of hubris").

[256] Stephen I. Vladeck, *The Espionage Act and National Security Whistleblowing After* Garcetti, 57 AM. U. L. REV. 1531, 1535 (2008).

[257] *See* 5 U.S.C. § 2302(b)(8)(A)-(B) (2012).

[258] *See, e.g.*, American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, § 1553(a), 123 Stat. 115, 297; *see also* 5 U.S.C. § 2303(a); 6 U.S.C. § 1142(a)(1) (2012); 10 U.S.C. § 2409(a) (2012); 15 U.S.C. § 2087(a) (2012); 18 U.S.C. § 1514A(a) (2012). Relatedly, some laws protect "good faith" reports of a violation of a law or regulation. *See, e.g.*, 46 U.S.C. § 2114(a)(1) (2006). Other federal whistleblower protection laws protect employees who object or refuse to participate in activities they reasonably believe violate federal law. *See, e.g.*, 15 U.S.C. § 2087(a); 21 U.S.C. § 399d(a) (2012); 29 U.S.C. § 218c(a) (2012); 49 U.S.C. § 30171(a) (2006).

[259] *See, e.g.*, 15 U.S.C. § 2651.

[260] *See, e.g.*, 42 U.S.C. § 5851(a)(1)(A) (2006).

[261] 5 U.S.C. § 2302(b)(9). Covered employees who refuse to obey an order to violate a law are also protected. *Id.*

[262] CONG. RESEARCH SERV., RL33918, THE WHISTLEBLOWER PROTECTION ACT: AN OVERVIEW 1 (2007), *archived at* http://perma.cc/FVS7-WRHF.

[263] 5 U.S.C. § 2302(b)(8)(A).

appears on its face to apply only to government employees.[264] Second, government employees in national security agencies are generally excluded from the WPA's coverage.[265] Third, federal employees covered under the WPA will find themselves without protection under the WPA if they disclose classified information that is marked as an executive order and regarding defense or foreign affairs to anyone except the Inspector General (IG) or Special Counsel.[266]

Under the WPA, federal employees may not give classified information to the IG or Special Counsel when they are reporting a violation of "any law, rule, or regulation," or "gross mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety."[267] In addition, the IG and Special Counsel can share these reports with only the National Security Advisor and the House and Senate Permanent Select Committees on Intelligence.[268] While this limited oversight may help in some cases, it is likely to be completely ineffective when the highest government officials have already approved of the alleged illegal activity.[269] And as observed above, IGs do not offer an independent check on executive power because they are under the command and authority of their respective agency heads and subject to removal by the President. Furthermore, there is evidence that some agencies use IGs to retaliate against whistleblowers "by initiating IG investigations about whistleblowers."[270]

Recognizing that the WPA provided essentially no protection to intelligence community employees,[271] Congress passed the Intelligence Community Whistleblower Protection Act of 1998 (ICWPA).[272] The ICWPA protects employees of federal intelligence agencies, as well as contractors for any of those agencies, who disclose classified information directly to Congress.[273] Hindered by arguments from the executive branch that the protection for such disclosures amounted to an unconstitutional infringement on that branch's

[264] *Id.*

[265] *Id.*

[266] *Id.* (exempting employees from protection if the information reported is specified by executive order to be kept secret in the interest of national defense).

[267] *Id.* § 2302(b)(8)(B) (containing no exception for classified information).

[268] *Id.* § 1213(j).

[269] Vladeck, *supra* note 256, at 1544 ("This problem could occur in cases where the 'unlawful secret' was been approved at the highest levels of the federal government.").

[270] *See* MELISSA GOODMAN ET AL., ACLU, DISAVOWED: THE GOVERNMENT'S UNCHECKED RETALIATION AGAINST NATIONAL SECURITY WHISTLEBLOWERS 9 (2007), *archived at* http://perma.cc/LCG9-L34T.

[271] Thomas Newcomb, *In from the Cold: The Intelligence Community Whistleblower Protection Act of 1998*, 53 ADMIN. L. REV. 1235, 1237-40 (2001).

[272] This act was codified in 50 U.S.C. § 403(q) (2006) for the CIA; for all other intelligence organizations, it was codified under 5 U.S.C. app. 3 § 8H.

[273] 50 U.S.C. § 403q(d)(5)(D).

power to withhold confidential communications and national security information, the statute provides much less protection than the WPA does for federal employees generally.[274]

The ICWPA protects a government employee only if he discloses a matter of "urgent concern," narrowly defined to include "a serious or flagrant" violation of law or executive order, a false statement to Congress (or willful withholding of information from Congress), or a reprisal against a person who reported a matter of urgent concern.[275] Bowing to the executive's concerns, the legislation does not permit intelligence community employees to make direct disclosures to Congress.[276] Instead, the employees must make disclosures to the appropriate Inspector General,[277] who in turn must notify the relevant agency head.[278] Furthermore, the employee may report directly to the congressional intelligence committees only if several onerous conditions are met.[279]

Notably, unlike the WPA, the ICWPA provides no legal remedy for retaliation against a covered employee. The ICWPA specifically states that "[a]n action taken by the Director or the Inspector General . . . shall not be subject to judicial review."[280] Agencies can, and often do, try to stop a whistleblower from talking to Congress "by claiming Congress is not authorized to hear what the whistleblower has to say."[281] Thus, absent any enforcement mechanism, the ICWPA arguably fails to provide any real protection to national security whistleblowers.

Another common criticism of the current whistleblower protection statutes is that they do not protect covered employees from security clearance-related retaliation.[282] Despite the seemingly expansive statutory language regarding what qualifies as a personnel action, courts have held that an agency's decision to revoke or suspend security clearance is not reviewable.[283] Thus, the

[274] *See generally* Newcomb, *supra* note 271.

[275] 50 U.S.C. § 403q(d)(5)(G)(i).

[276] *Id.* § 403q(d)(5)(A).

[277] *Id.* ("An employee of the Agency, or of a contractor to the Agency, who intends to report to Congress a complaint or information with respect to an urgent concern may report such complaint or information to the Inspector General.").

[278] *Id.* § 403q(d)(5)(B).

[279] *Id.* § 403q(d)(5)(D) (explaining that an employee may report to intelligence committees if the Inspector General does not find the disclosure credible, the employee gives written notice to Inspector General, and obtains instructions from Director on how to contact them).

[280] *Id*. § 403q(d)(5)(F).

[281] *See* Goodman et al., *supra* note 270, at 10.

[282] Moberly, *supra* note 67, at 102.

[283] Gargiulo v. Dep't of Homeland Sec., 727 F.3d 1181, 1185 (Fed. Cir. 2013); Robinson v. Dep't of Homeland Sec., 498 F.3d 1361, 1364 (Fed. Cir. 2007). The Federal Circuit has recently held that government agency determinations concerning the eligibility of an employee to occupy a "sensitive" national security position are not reviewable, even if that

revocation of security clearance has become a common tactic allowing agencies to retaliate against lawful whistleblowers with impunity.[284] Allowing agencies to alter an employee's security clearance provides agencies with a back door way to effectively fire or blacklist employees who blow the whistle. Reformers have called for the implementation of fair internal due process rights, which can be reviewed by the Merit Systems Protection Board, to provide a mechanism for resolving adverse clearance judgments, and also the option of an independent appeal to those decisions to a forum free from institutional conflict.[285]

Members of the armed forces are protected under the Military Whistleblower Protection Act of 1988, which offers the same sort of limited protection that members of the intelligence community have. The Act excludes communications that are "unlawful," without defining the term,[286] thus leaving open the possibility that any unauthorized disclosure of classified information would not be covered. At the same time, the law protects from retaliation members of the military who report their reasonable belief of illegal action as well as "[g]ross mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety."[287] These disclosures must be made to a Member of Congress, the IG, or other designated officials to be protected.[288] It is unclear as a matter of statutory construction whether these disclosures are protected if they include classified information given the exclusion of "unlawful" disclosures in another part of the statute.

The executive branch has continued to oppose attempts to remove some of the limitations inherent in the WPA and ICWPA, as applied to intelligence community employees. As originally drafted, the Whistleblower Protection Enhancement Act (WPEA), which passed in 2010, would have amended the WPA to extend whistleblower protections to national security employees and

position does not involve access to classified information. Kaplan v. Conyers, 733 F.3d 1148 (Fed. Cir. 2013).

[284] *See* Goodman et al., *supra* note 270, at 15 ("This means that even if an employee is covered by the WPA, the employee is unprotected if an agency retaliates not by suspending or firing the employee outright but by first revoking her security clearance and then firing her because she no longer a has clearance. There is no independent court or administrative body that can review whether a suspension or revocation of a security clearance is retaliatory.").

[285] SHANNA DEVINE ET AL., GOV'T ACCOUNTABILITY PROJECT, WHISTLEBLOWER WITCH HUNT: THE SMOKESCREEN SYNDROME 39 (2010), *archived at* http://perma.cc/38Q7-H4Q5 ("Legitimate reform requires that – whistleblower rights extending to protect against security clearance retaliation; fair internal agency due process rights to resolve proposed adverse clearance judgments; and independent appeal of those decisions to a forum free from institutional conflict of interest.").

[286] 10 U.S.C. § 1034(a)(2) (2012).

[287] *Id.* § 1034(c)(2).

[288] *Id.* § 1034(b)(B).

contractors.[289] The original legislation proposed in 2007 would also have made decisions to revoke or suspend security clearance actionable and would have permitted employees to bring actions in any federal court.[290] The President opposed this legislation,[291] repeating the common refrain that the expansion of whistleblower protection to national security employees who disclose classified information to Congress without authorization from the executive branch would jeopardize national security and would impede the President's coordination function.[292] The Executive Office further objected to the portions of the legislation that would prohibit the government from invoking the state secrets privilege, and more generally argued that allowing administrative and judicial review of executive branch security clearance determinations was inconsistent with the executive branch's discretion in that area.[293] The letter also objected to the WPEA's expansion of protected disclosures, which it claimed would lead to frivolous lawsuits.[294]

Congress ultimately acceded to the executive's arguments to exclude national security employees and contractors from the WPEA, and President Obama signed the legislation into law. The timing of Congress's decision to strip the bill of protections for these individuals corresponded with the unauthorized leak of hundreds of thousands of classified diplomatic cables to the website WikiLeaks, allegedly by Manning. Although Manning would have received no protection under the WPEA, some believe the massive leak was partially responsible for the bill's failure.[295] Congress has also excluded members of the intelligence community from the recently adopted pilot program passed as part of the National Defense Authorization Act of 2013.[296]

Although the WPEA does not cover most members of the intelligence community, President Obama released Presidential Policy Directive 19 (PPD-19) in an effort to extend some of the WPEA protections to national security employees.[297] PPD-19 prohibits retaliation against any employee with access to national security information who reports a reasonable belief of waste, fraud, or abuse to someone in his chain of command, the IG of his agency, the

[289] CONG. RESEARCH SERV., *supra* note 262, at 17.

[290] Statement of Administration Policy, H.R. 985 – Whistleblower Protection Enhancement Act of 2007 (Mar. 13, 2007), *archived at* http://perma.cc/XHS4-YXLC.

[291] *Id.*

[292] *Id.*

[293] *Id.*

[294] *Id.*

[295] Miranda Leitsinger, *As Manning Heads to Trial over Wikileaks, New Push for Whistleblower Protections*, MSNBC (Dec. 16, 2011, 6:54 AM), http://usnews.msnbc.msn.com/_news/2011/12/16/9483316-as-manning-heads-to-trial-over-wikileaks-new-push-for-whistleblower-protections, *archived at* http://perma.cc/ZFV7-5LFC.

[296] National Defense Authorization Act for Fiscal Year 2013, Pub. L. No. 112-239, § 828(a)(1), 2013 U.S.C.C.A.N. (126 Stat.) 1632, 1837-41.

[297] Presidential Policy Directive/PPD-19, *supra* note 252.

Director of National Intelligence, to the IG of the Intelligence Community, or anyone designated by these officials to receive such disclosures.[298] Although this is a laudable measure, it lacks the force of a statute, relies on the individual agencies for implementation, and appears to offer more procedural than substantive protections.[299] PPD-19 gives aggrieved employees the right to appeal to a three-member panel of IGs, but the decision of that panel is subject to review by the agency head, thereby potentially mitigating much of the benefit of the outside review. PPD-19 makes clear that it "is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable in law or equity by any party against the United States" or any other agency or person.[300] Furthermore, PPD-19 does not give employees the right to external review – such as in an Article III court – of any personnel action, and offers no protection to employees who disclose information to a congressional committee or to the media.[301] Finally, PPD-19 refers only to "officer[s] or employee[s] of a Covered Agency," and therefore appears to give no protection to government contractors.[302]

B. *Criminal Sanctions*

In addition to constitutional and military treason, government insiders who engage in the unauthorized dissemination of national security information can face a range of potential criminal charges. The existing law does not do a particularly good job of distinguishing traitors, spies, whistleblowers, and other leakers.

1. Constitutional Treason

As Chief Justice Marshall said, "there is no crime which can more excite and agitate the passions of men than treason."[303] Since the founding of the nation, commentators and politicians on both sides of the aisle have labeled the leaking and publication of national security information as treason.[304]

---

[298] *Id.*

[299] For criticism of the Presidential Policy Directive, see Owen Dunn, *Presidential Policy Directive on Whistleblowers Draws Criticism*, WHISTLEBLOWER'S PROTECTION BLOG (Oct. 16, 2012), http://www.whistleblowersblog.org/2012/10/articles/news-1/presidential-policy-directive-on-whistleblowers-draws-criticism/#more, *archived at* http://perma.cc/5UJN-YVMC.

[300] Presidential Policy Directive/PPD-19, *supra* note 252.

[301] *See* Elizabeth Goitein, *A Mixed Message for National Security Whistleblowers*, HUFFINGTON POST (Oct. 22, 2012), http://www.huffingtonpost.com/elizabeth-goitein/obama-whistleblowers_b_1989629.html, *archived at* http://perma.cc/SM7C-G8KL.

[302] Presidential Policy Directive/PPD-19, *supra* note 252.

[303] *Ex parte* Bollman, 8 U.S. (4 Cranch) 75, 125 (1807).

[304] SCHOENFELD, *supra* note 6, at 73-74 (writing that Thomas Paine was accused of treason for disclosing in his *Crisis* pamphlets that the French were secretly financing American forces in the Revolution); Editorial, *Snowden's Disclosures Do Not Amount to*

Although it is sometimes unclear whether policymakers mean that the leakers are guilty of treason, or whether they are simply using the loaded words "treason" and "traitor" to condemn the disclosures. The frequency with which this label is thrown around begs the question whether leakers could be convicted of treason.

Treason is the only crime specified in the Constitution.[305] Article III, Section 3 provides: "Treason against the United States, shall consist only in levying War against them, or in adhering to their Enemies, giving them Aid and Comfort. No person shall be convicted of Treason unless on the Testimony of two Witnesses to the same overt Act, or on Confession in open Court."[306]

Treason can take two forms: (1) levying war against the United States, or (2) adhering to the enemy.[307] No one has been charged with the first type of treason since the end of the Civil War,[308] and while the second type "has achieved a considerably longer and more useful existence,"[309] only one person has been charged with treason since World War II.[310] Since that time, the government has relied more heavily on other charges to punish those who threaten the security of the nation.[311] Nevertheless, given the government's

Treason, N.Y. TIMES, June 11, 2013, at A26 (observing that both Republican House Speaker John Boehner and Democratic Senator Diane Feinstein have accused Edward Snowden of treason); Adam Liptak, *In Rulings, Spy vs. Leaker*, N.Y. TIMES, Aug. 3, 2013, at A1 (writing that President Richard Nixon called the publication of the Pentagon Papers "treasonable"); Chris Mondics, *Santorum Says NSA Leakers Committed Treason*, PHILA. INQUIRER, Aug. 12, 2006, at A9.

[305] United States v. Greathouse, 26 F. Cas. 18, 21 (C.C.N.D. Cal. 1863) (No. 15,254).

[306] U.S. CONST. art. III, § 3, cl. 1. Although the Constitution defines the crime of treason, Congress determines the applicable punishment. *See* 18 U.S.C. § 2381 (2012) ("Whoever, owing allegiance to the United States, levies war against them or adheres to their enemies, giving them aid and comfort within the United States or elsewhere, is guilty of treason and shall suffer death, or shall be imprisoned not less than five years and fined under this title but not less than $10,000; and shall be incapable of holding any office under the United States.").

[307] *See* 18 U.S.C. § 2381.

[308] *See Greathouse*, 26 F. Cas. at 22; Captain Jabez W. Loane, IV, *Treason and Aiding the Enemy*, 30 MIL. L. REV. 43, 58 (1965).

[309] Loane, IV, *supra* note 308, at 58.

[310] *See* Eric Litchblau, *American in Qaeda Tapes Accused of Treason*, N.Y. TIMES, Oct. 12, 2006, at A22 (reporting the 2006 treason indictment of Adam Yahiye Gadahn based on his participation in several Al Qaeda video tapes in which he expresses his support for terrorism, as the first of its kind "in more than a half-century"). Gadahan remains at large and is currently listed as one of the FBI's most wanted terrorists. *Wanted by the FBI: Adam Yahiye Gadahn*, FBI (2013), http://www.fbi.gov/wanted/wanted_terrorists/adam-yahiye-gadahn, *archived at* http://perma.cc/YDV4-V8DF.

[311] Willard Hurst, *Treason in the United States*, 58 HARV. L. REV. 806, 806 (1945) ("[A]fter the nineteenth century the executive and legislative branches no longer considered the treason charge as the principal bulwark of state security."). In *Cramer v. United States*, the seminal case on treason, the Supreme Court opined that as a nation "[w]e have managed

decision to charge an American-born terror propagandist with treason and to prosecute Bradley Manning with the similar charge of aiding the enemy, it is possible that the government will bring treason charges more frequently in the future.[312]

The second type of treason requires two separate elements: (1) "adhering to the enemy," and (2) the provision of "aid and comfort" to the enemy.[313] The Supreme Court has held that the crime of treason requires both overt acts and a specific intent to betray.[314] These two requirements are "packed with controversy and difficulties,"[315] and the Supreme Court has made clear that both elements are necessary for proving treason:

> A citizen intellectually or emotionally may favor the enemy and harbor sympathies or convictions disloyal to this country's policy or interest, but so long as he commits no act of aid and comfort to the enemy, there is no treason. On the other hand, a citizen may take actions, which do aid and comfort the enemy—making a speech critical of the government or opposing its measures, profiteering, striking in defense plants or essential work, and the hundred other things which impair our cohesion and diminish our strength—but if there is no adherence to the enemy in this, if there is no intent to betray, there is no treason.[316]

Whether the defendant has committed an overt act that provides aid and comfort to the enemy is a question of law to be determined by a court.[317]

---

to do without treason prosecutions to a degree that probably would be impossible except while a people was singularly confident of external security and internal stability." 325 U.S. 1, 26 (1945).

[312] Furthermore, as one scholar has observed, "[t]he recent lull in [treason] prosecutions should not blind us to the peril that the law of treason conceals." Tom Bell, *Treason, Technology, and Freedom of Expression*, 37 ARIZ. ST. L.J. 999, 1002 (2005).

[313] *See* Kawakita v. United States, 343 U.S. 717, 736 (1952); *Cramer*, 325 U.S. at 29. The government must also prove that the defendant owed "allegiance" to the United States. 18 U.S.C. § 2381 (2012). U.S. citizens (including dual citizens) and resident noncitizens all owe a duty of allegiance to the United States. Bell, *supra* note 312, at 1011 (citing *Kawakita*, 343 U.S. at 736; Carlisle v. United States, 83 U.S. (16 Wall.) 147, 155 (1873)).

[314] *Cramer*, 325 U.S. at 29. Although court opinions are quite clear that treason requires the specific intent to betray the United States, and not just a general intent to commit the overt acts, some scholars disagree. *See, e.g.*, JUSTIN MILLER, HANDBOOK OF CRIMINAL LAW 502 (1934) ("In order that the crime of treason be committed there must be an intent. However no specific intent is required. It is sufficient that the defendant intended to do the prohibited act.").

[315] *Cramer*, 325 U.S. at 46-47 ("The framers' effort to compress into two sentences the law of one of the most intricate of crimes gives a superficial appearance of clarity and simplicity which proves illusory when it is put to practical application.").

[316] *Id.* at 29; *see also Kawakita*, 343 U.S. at 736; Haupt v. United States, 330 U.S. 631, 634-35 (1947).

[317] *See Haupt*, 330 U.S. at 635-36 (holding that the acts alleged were sufficient to sustain the finding of an overt act, provided the jury credit the evidence); *Cramer*, 325 U.S. at 34

Unless the defendant testifies in open court, any prosecution for treason constitutionally requires two witnesses who can testify that the defendant committed the allegedly treasonous actions.[318] Witnesses are not required, however, to demonstrate that the defendant had the specific intent to betray the country; after all, witnesses cannot read someone's mind.[319]

To satisfy the overt act requirement, the government does not have to show that the attempt to assist the enemy was substantial, complete, effective, or successful.[320] 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,[321] or, as in one case, that the information was even received.[322]

The government, however, does, have to prove that the individual who transmitted information gave aid and comfort to an "enemy" of the United States.[323] The Constitution provides no guidance for defining "enemy" within the Treason Clause,[324] but the British statute upon which the Clause was modeled had been interpreted broadly such that "enemy" was not limited by formal declarations of war against nation states.[325] The Constitution is also silent on whether a formal declaration of war is required,[326] yet the few

("The very minimum function that the overt act must perform in a treason prosecution is that it show sufficient action by the accused, in its setting, to sustain a finding that the accused actually gave aid and comfort to the enemy.").

[318] U.S. CONST. art. III, § 3, cl. 1.

[319] *Cramer*, 325 U.S. at 31.

[320] *See Kawakita*, 343 U.S. at 738-39; *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.").

[321] Chandler v. United States, 171 F.2d 921, 941 (1st Cir. 1948).

[322] *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).

[323] *Cramer*, 325 U.S. at 29.

[324] The term appears twice in the Constitution. U.S. CONST. art. III, § 3, cl. 3 (using the term "Enemies" in the definition of treason); *id.* amend. XIV, § 3 (prohibiting any person who has engaged in insurrection or rebellion or aided the enemy from running for public office).

[325] Carlton F.W. Larson, *The Forgotten Constitutional Law of Treason and the Enemy Combatant Problem*, 154 U. PA. L. REV. 863, 915-16 (2006) (defining the English statute on which the Constitution's Treason Clause was predicated as broad and "not limited only to those foreign states against which England had declared war"); *see* Treason Act, 1351, 25 Edw. 3, c. 2 (Eng.) (declaring it to be treasonous "if a Man do levy War against our Lord the King in his Realm, or be adherent to the King's Enemies in his Realm, giving to them Aid and Comfort in the Realm, or elsewhere").

[326] U.S. CONST. art. III, § 3, cl. 1.

decisions to address the matter[327] limit the term "enemy" to "subjects or citizens of a foreign State at war with our own."[328] Thus, once war has been declared against the United States, a foreign power's subjects, military, agents, and spies are enemies of the United States until the cessation of hostilities.[329] For example, the Rosenbergs, who famously gave nuclear secrets to the Soviet Union in the 1950s, were not charged with treason because the United States was not at war with Russia at that time.[330] In the context of the United States' struggle against terrorism, however, organizations such as Al Qaeda might qualify as "enemies" under the Treason Clause.[331]

Assuming Al Qaeda is an enemy under the Treason Clause, the transmission of classified information directly to Al Qaeda would plainly satisfy the "aid and comfort" to the enemy requirement.[332] It does not matter whether the information was useful to the enemy or its disclosure harmful to the United States; indeed, even entirely futile attempts to aid the enemy can be treason.[333] It is less clear whether the government could bring treason charges against someone who disseminates classified information directly to the public (perhaps through a personal blog) or through some sort of media intermediary (such as WikiLeaks or the *New York Times*) with the asserted intent of

[327] *See* Larson, *supra* note 325, at 917 n.270 ("A consistent line of cases holds that a United States citizen who remains in enemy territory after the initiation of hostilities may be treated as an enemy, at least insofar as seizure of his property by the military in wartime is concerned.").

[328] The Prize Cases, 67 U.S. (2 Black) 635, 672 (1863).

[329] United States v. Fricke, 259 F. 673, 675-76 (S.D.N.Y. 1919) (holding that upon declaration of war with the United States anyone attempting to contravene the United States's counterpursuance of war was an enemy of the United States); Benjamin A. Lewis, Note, *An Old Means to a Different End: The War on Terror, American Citizens . . . and the Treason Clause*, 34 HOFSTRA L. REV. 1215, 1227 (2006). The formal war requirement, however, is not absolute. *See The Prize Cases*, 67 U.S. at 666-67 (holding that a civil war begins with an insurrection, so war is never formally declared, but instead arises "by its accidents" and under certain conditions). During the Civil War, for instance, President Abraham Lincoln was permitted to establish a Union blockade of Confederate ports absent a formal declaration of war because, as per the international laws of war, the Confederate rebels had "cast off their allegiance and made war on their government." *Id.* at 671, 674.

[330] *See* United States v. Rosenberg, 195 F.2d 583, 588-90, 610-11 (2d Cir. 1952) (responding to an argument by the Rosenbergs that they should have been prosecuted for treason and hence afforded the protections of that charge by holding that "an essential element of treason, giving aid to an 'enemy,' is irrelevant to the espionage offense").

[331] *See* Larson, *supra* note 325, at 920 (arguing that Al Qaeda, unlike Russia during the Cold War, would likely be classified as an enemy because "Al Qaeda has engaged in violent, war-like attacks on the United States," whereas Russia and the United States were never in "open war").

[332] *See* Chandler v. United States, 171 F.2d 921, 941 (1st Cir. 1948) (holding that conveying military information "would be a completed act of aid and comfort").

[333] Haupt v. United States, 330 U.S. 631, 644 (1947).

informing the American public.[334] Unlike Uniform Code of Military Justice Article 104, the Treason Clause does not contain language indicating that aiding the enemy can happen "directly or indirectly."[335] A defendant might argue that aiding the enemy under the Treason Clause requires the government to demonstrate that the individual disclosed the information to the public or through an intermediary with the intent that it would reach the enemy.[336]

The government is likely to respond that the subjective intent of the defendant is irrelevant in determining whether the defendant provided aid and comfort to the enemy.[337] Instead, it might argue, the defendant is assumed to be aware that the enemy can access anything revealed to the public at large.[338] The Court's treason cases do not expressly require one to act with the enemy's consent of the enemy or have any sort of direct relationship with the enemy, although in all of the cases the defendants did, in fact, serve as agents of the enemy.[339] Requiring some sort of direct relationship, agreement, or arrangement with the enemy would seem essential to avoid a dramatic expansion of the Treason Clause.[340] Any number of actions can "aid" the enemy – from sabotaging a weapons plant to criticizing the United States – but unless this act is done at the behest or at least in cooperation with the enemy, it does not seem correct to call this act "treason."[341]

Regardless of whether the defendant's subjective intent is relevant in determining whether the "aid and comfort" requirement is met, this intent might be relevant in determining whether the adherence to the enemy

---

[334] *See* Marcy Wheeler, *Whistleblowing Now Akin to Treason*, SALON (Apr. 17, 2013, 12:20 PM), http://www.salon.com/2013/04/17/obama_administration_equates_whistleblowing_to_spying_partner, *archived at* http://perma.cc/Q3A7-TBWN.

[335] *Compare* Uniform Code of Military Justice, 10 U.S.C. § 904 (2012) (defining the military crime of aiding the enemy), *with* U.S. CONST. art. III, § 3, cl. 1.

[336] *See supra* notes 313-16 and accompanying text (explaining the mens rea requirement that inheres in the adherence element of treason).

[337] Wheeler, *supra* note 334 (quoting the government as arguing that providing information to the *New York Times* was worse than selling information to an enemy because "every foreign adversary stood to benefit from the defendant's unauthorized disclosure").

[338] *See* William Saletan, *Truth Is Treason*, SLATE (July 31, 2013, 11:45 AM), http://www.slate.com/articles/news_and_politics/frame_game/2013/07/did_bradley_manning_aid_the_enemy_the_prosecution_s_case_was_preposterous.html, *archived at* http://perma.cc/U6VQ-BNHL (explaining that the Government based its argument that Manning "aided the enemy" on the idea "that the world includes our enemies, and that they use the Internet").

[339] *See* Bell, *supra* note 312, at 1014-15.

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

[341] *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.").

requirement is met.[342] The Court has said that the requisite intent can be "inferred from the overt acts themselves, from the defendant's own statements of his attitude toward the war effort, and from his own professions of loyalty to [the enemy]."[343] Some scholars have argued that this language leaves unclear whether the crime of treason simply requires general criminal intent to perform the overt act at issue – by permitting intent to betray to be inferred from the overt acts themselves – or whether the government must demonstrate a more specific intent to betray.[344]

Eminent legal scholar Charles Warren, who served as an assistant attorney general during World War I, argued that a specific intent to betray is not necessary in most cases.[345] He explained that "if . . . a person intends to do and actually does specific acts the natural and probable consequences of which are the giving of aid and comfort to the enemy, then he intends to commit treason, within the purview of the law."[346] To support his argument, Warren relied on Supreme Court decisions in which defendants claimed that they intended only to make money and did not intend to give aid to the nation's enemies.[347] Showing little patience for the defendants in such cases, the Court relied on the general principle of law that a defendant cannot avoid civil or criminal liability by pretending that they did not know what the recipient of their support was going to do with that support.[348] Furthermore, some lower courts have been clear that defendants who clearly aided the enemy cannot avoid a treason conviction by arguing that they believed it would be for the good of the nation in the long run.[349] For example, the First Circuit has held that a defendant who gives the enemy advance information about a planned invasion cannot avoid a treason charge based on his sincere belief that it would be best for the country to be defeated and withdraw early from the conflict.[350]

---

[342] *Id.* at 1023 (observing that it is not the overt act element, but rather the adhering element that might prevent a treason conviction for expressive activities).

[343] Kawakita v. United States, 343 U.S. 717, 742-43 (citing Haupt v. United States, 330 U.S. 631, 642 (1947); Cramer v. United States, 325 U.S. 1, 31 (1945)).

[344] *Compare* Loane, IV, *supra* note 308, at 78 (explaining that *Cramer*'s language, stating that intent can be inferred from the overt acts themselves, indicates that treason requires "something less" than specific intent to betray), *with* Hurst, *supra* note 311, at 826-27 (acknowledging the tension in the cases but concluding that specific intent is required).

[345] *See* Charles Warren, *What Is Giving Aid and Comfort to the Enemy*, 27 YALE L.J. 331, 344 (1918).

[346] *Id.*

[347] *Id.* ("[The defendant] cannot be permitted to stand on the nice metaphysical distinction that, although he knows that the purchaser buys the goods for the purpose of aiding the rebellion, he does not sell them for that purpose. The consequences of his acts are too serious and enormous to admit of such a plea." (quoting Hanauer v. Doane, 79 U.S. (12 Wall.) 342, 347 (1870)) (internal quotation marks omitted)).

[348] Sprott v. United States, 87 U.S. (20 Wall.) 459, 463-64 (1874).

[349] Chandler v. United States, 171 F.2d 921, 943 (1st Cir. 1948).

[350] *Id.* at 944.

But the arguments that specific intent is irrelevant are potentially inconsistent with the Court's decision in *Haupt v. United States*, which affirmed the treason conviction of the father of a German saboteur during World War II.[351] There, the Court suggested that it is appropriate to permit the jury to consider whether the defendant had benign motives for extending aid to the enemy.[352] 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."[353] 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.[354] The jury in that case ultimately found the father guilty.[355] The Court affirmed the conviction, reasoning that the jury could have reasonably determined that the father did have intent to betray the United States, given the several statements he made indicating his "adherence to the German cause."[356] *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 conclude that the defendant acted with a specific intent to betray.

The Supreme Court has held that the Treason Clause does not limit the United States' ability to punish other conduct that has the effect of undermining our national security and cohesion.[357] The lower courts have accepted this conclusion,[358] but it is hardly a frivolous argument that at least some portions of the Espionage Act are unconstitutional.[359] In the famous Rosenberg espionage case, Justice Black dissented from a denial of certiorari where the defendants had argued that they could not be convicted for the act of transmitting secrets to the Soviet Union unless the government satisfied the procedural requirements of the Treason Clause.[360]

---

[351] Haupt v. United States, 330 U.S. 631, 641 (1947).

[352] *Id.*

[353] *Id.*

[354] *Id.*

[355] *Id.* at 644.

[356] *Id.* at 641-42.

[357] *See* Cramer v. United States, 325 U.S. 1, 45 & n.52 (1945) ("[T]he treason offense is not the only nor can it well serve as the principal legal weapon to vindicate our national cohesion and security.").

[358] *See, e.g.*, United States v. Kim, 808 F. Supp. 2d 44, 49-51 (D.D.C. 2011) (rejecting the defendant's "compelling and eloquent argument" that he "must be charged with treason or nothing at all").

[359] *See* Paul Crane, *Did the Court Kill the Treason Charge?: Reassessing* Cramer v. United States *and Its Significance*, 36 FLA. ST. L. REV. 635, 694-95 (2009).

[360] Rosenberg v. United States, 346 U.S. 273, 300 (1953) (Black, J., dissenting) (arguing

Not surprisingly, the few scholars to address the issue have expressed concern that the potentially staggering breadth of the Treason Clause conflicts with the First Amendment.[361] The Supreme Court, which last decided a treason case in 1947, has not had the opportunity to consider this issue in light of modern First Amendment principles that developed in the decades following World War II.[362] Although propagandists employed by our enemies like Ezra Pound and Iva Toguri d'Aquino, also known as "Tokyo Rose," have been prosecuted for treason, never in the history of this nation has the government prosecuted someone for treason for leaking or publishing secrets to the press.[363]

2. Military Treason

Article 104 of the Uniform Code of Military Justice is similar to the constitutional crime of treason in some ways, but it is an entirely separate offense.[364] Manning was charged with violating this provision by providing approximately 700,000 government documents to WikiLeaks that were in turn allegedly read by Al Qaeda.[365] Manning was acquitted of an article 104 charge after a full bench trial.[366]

The law defines the crime as:

> 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.[367]

that the petition for certiorari should have been granted to review the fairness of the trial and the government's right "to try these defendants except under the limited rules prescribed by the Constitution defining the offense of treason").

[361] Bell, *supra* note 312, at 1040 (arguing that convictions involving treasonous expression must be limited to employees of U.S. enemies to avoid conflict with the First Amendment).

[362] *Id.* at 1030 (arguing that the Supreme Court's post–World War II First Amendment decisions indicate "that the law of treason violates the First Amendment").

[363] SCHOENFELD, *supra* note 6, at 80-81.

[364] *See* 10 U.S.C. § 904 (2012).

[365] Charlie Savage, *Soldier Admits Providing Files to WikiLeaks*, N.Y. TIMES, Mar. 1, 2013, at A1.

[366] Charlie Savage, *Manning Found Not Guilty of Aiding the Enemy*, N.Y. TIMES, July 31, 2013, at A1.

[367] 10 U.S.C. § 904.

Like constitutional treason, violations of article 104 are punishable by death.[368]

Although article 104 is frequently compared to treason, there are significant differences.[369] Most obviously, article 104 does not prohibit the "levying war" type of treason or contain the evidentiary requirement of either the testimony of two witnesses to the overt act or a confession in open court.[370] Another important difference between treason and article 104 is that treason requires that the defendant have a duty of allegiance to the United States, and article 104 does not.[371] Despite the obvious differences between treason and article 104, military courts appear to treat article 104 as the rough equivalent of treason.[372] They frequently rely on civilian treason cases and even are mindful of constitutional treason's two-witness rule.[373]

Unlike constitutional treason, article 104(2) expressly prohibits any communications with the enemy.[374] The statute is not limited to disclosures of classified information; it also does not require the government to demonstrate that the disclosure was harmful to the United States or useful for the enemy.[375] Furthermore, the communications can be "direct or indirect."[376] The explanatory notes accompanying the law make clear that the provision is intentionally broad: "The intent, content, and method of the communication, correspondence, or intercourse are immaterial. No response or receipt by the enemy is required."[377] Indeed, the Manning prosecution made clear that it would have considered bringing this charge even if Manning had disclosed

[368] *Id.*

[369] *Compare id.* (defining the military crime of aiding the enemy), *with* U.S. CONST. art. III, § 3, cl. 1 (defining the criminal offense of treason).

[370] 10 U.S.C. § 904.

[371] *Id.* This point is not free of debate. For a thorough discussion of whether article 104 requires allegiance, see Michael J. Lebowitz, *A Question of Allegiance: Choosing Between Dueling Versions of "Aiding the Enemy" During War Crimes Prosecution*, 67 A.F. L. REV. 131, 138 (2011).

[372] Loane, IV, *supra* note 308, at 78.

[373] *Id.* at 78-79. It is notable that in closing arguments, the prosecutor in the Manning trial declared that Manning "was not a whistle-blower. He was a traitor, a traitor who understood the value of compromised information in the hands of the enemy and took deliberate steps to ensure that they, along with the world, received it." Charlie Savage, *In Closing Argument, Prosecutor Casts Soldiers as 'Anarchist' for Leaking Archives*, N.Y. TIMES, July 25, 2013, at A14.

[374] 10 U.S.C. § 904(2).

[375] *See* MANUAL FOR COURTS-MARTIAL, UNITED STATES pt. IV, ¶ 28.c.(6)(a) (2012) ("No unauthorized communication, correspondence, or intercourse with the enemy is permissible. The intent, content, and method of the communication, correspondence, or intercourse are immaterial.").

[376] *Id.*

[377] *Id.* pt. IV, ¶ 28.b.(6)(a).

secrets directly to the *New York Times* instead of WikiLeaks,[378] and our enemies are highly likely to read our major newspapers.

As with constitutional treason, defendants facing article 104(2) charges have argued that the government must demonstrate that they acted with the specific intent of aiding the enemy.[379] The Supreme Court has never addressed this issue, but in *United States v. Batchelor*, the Court of Military Appeals held that specific intent was not required.[380] In that case, the accused was a prisoner of war who made speeches and public broadcasts within his prison camp condemning the United States, and also directly gave information about other prisoners to his captors.[381] The defendant was convicted of, among other things, communicating with the enemy without proper authority in violation of article 104(2).[382] The accused, who claimed that he believed he was acting in the best interest of the United States, argued that article 104(2) required the government to prove that he acted with the specific intent of harming his country or some other bad purpose.[383] Although the Court of Military Appeals recognized that "an offense which is so closely akin to treason and may be punished by a death sentence cannot be viewed as a 'public welfare' kind of dereliction,"[384] unlike treason, a specific criminal intent is not required. Instead, the court held, a finding of general criminal intent was sufficient.[385] In support of its conclusion, the court cited an early treatise that expressly distinguished a predecessor statute from treason on the grounds that the former did not require specific intent: "Thus correspondence with an enemy in regard to matters purely social or domestic, while lacking the animus of treason, would, unless duly authorized, constitute an offence."[386]

As the Manning trial revealed, it is unclear under what circumstances someone could be convicted under article 104(2) for disseminating information that ultimately reaches the enemy. Article 104(2) requires that a defendant "knowingly" communicate with the enemy, "either directly or indirectly."[387] The Manning prosecutors argued that this standard is met whenever a defendant knows that his communication could reach the enemy, even if that

[378] Scott Shane, *New Evidence Expected in WikiLeaks Case*, N.Y. TIMES, Jan. 9, 2013, at A14. The *New York Times*, of course, did publish some of the materials Manning gave to WikiLeaks, but the paper did not receive the information from Manning directly. *Id.*

[379] *See, e.g.*, United States v. Batchelor, 22 C.M.R. 144, 157 (C.M.A. 1956).

[380] *Id.* at 158 ("Article 104(2) of the Code does not require specific criminal intent of any sort.").

[381] *Id.* at 150.

[382] *Id.* at 149.

[383] *Id.* at 156-57.

[384] *Id.* at 157 (quoting United States v. Doyle, 14 C.M.R. 3, 11 (C.M.A. 1954)).

[385] *Id.* at 158.

[386] *Id.* (quoting COLONEL WILLIAM WINTHROP, MILITARY LAW AND PRECEDENTS 630 n.78 (2d ed. 1920)).

[387] 10 U.S.C. § 904(2) (2012).

was not his intent.[388] Manning contended that the government must show that he intended to give intelligence to the enemy.[389] He cited an article 104(1) case in which the Court of Military Appeals expressed held that article 104 cannot be held to criminalize inadvertent, accidental, or negligent conduct,[390] lest a crime that carries the death penalty become a strict liability offense.[391] The trial court rejected this argument, and as a result, the trial focused on whether Manning knew or should have known, at the time he made his disclosures, whether Al Qaeda read WikiLeaks.[392]

The trial court ultimately ruled in favor of Manning on the article 104(2) charge, although it did not explain the basis for that decision.[393] As with constitutional treason, article 104(2) as applied to the indirect communication with the enemy raises a number of potential First Amendment "overbreadth and vagueness" issues that could have been the basis for the court's decision.[394]

3. Espionage Act and Other Criminal Statutes

At the outset, it is worth noting that Congress has not been able to pass the equivalent of an "Official Secrets Act" that would authorize the punishment of government insiders for the mere revelation of classification information,

[388] Matt Sledge, *Bradley Manning Aided the Enemy Because He Knew Al-Qaeda Uses the Internet, Prosecutors Charge*, HUFFINGTON POST (July 9, 2013, 7:31 AM), http://www.huffingtonpost.com/2013/07/09/bradley-manning-aiding-the-enemy_n_3543592.html, *archived at* http://perma.cc/K5QT-W263 ("The government's argument, then, is that any member of the military who leaks classified information with the knowledge that it will be posted on the Internet is aiding enemies of the United States.").

[389] Defense Motion to Dismiss the Specification of Charge I for Failure to State an Offense at 5-6, United States v. Manning (U.S. Army 1st Jud. Cir. Mar. 29, 2012), *archived at* http://perma.cc/UM6-7JAA ("The intent required is the intent to give the intelligence to the enemy.").

[390] United States v. Olson, 20 C.M.R. 461, 464 (C.M.A. 1955) ("[T]his offense does require a general evil intent in order to protect the innocent who may commit some act in aiding the enemy inadvertently, accidentally or negligently.").

[391] Defense Motion to Dismiss the Specification of Charge I for Failure to State an Offense, *supra* note 389, at 6.

[392] *See* Julie Tate, *Judge in Manning Case Declines to Dismiss Key Charge*, WASH. POST, July 19, 2013, at A4.

[393] Savage, *supra* note 366, at A1. Because Manning's lawyers requested specific findings only with respect to the charges for which he 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. Special Findings, United States v. Manning (U.S. Army 1st Jud. Cir. Aug. 15, 2013), *archived at* http://perma.cc/F5YA-XEKG.

[394] *See* Bell, *supra* note 312, at 1031-33, 1039 (arguing, in the parallel context of the Treason Clause, that its "overbreadth and vagueness" render it "constitutionally suspect" under the First Amendment); *see also* 10 U.S.C. § 904 (2012) (defining the Uniform Code of Military Justice crime of aiding the enemy).

regardless of its content, the harm it might have on national security, its value to public debate, and the intent of the leaker.[395] In vetoing one attempt to pass such legislation, President Bill Clinton observed that the law failed to strike the appropriate balance between the need to protect national security secrets and the need for the free flow of information in a democracy.[396] In his veto statement, Clinton explained that, "[a]lthough well intentioned, [the bill] is overbroad and may unnecessarily chill legitimate activities that are at the heart of a democracy."[397] Congress has considered similar legislation many times,[398] but every time these efforts have failed.

These proposed statutes have been criticized for several reasons. Some proposed legislation did not provide a defense for information that had been improperly classified, applied even to disclosures to Congress, and threatened the press with prosecution for either conspiracy to violate the proposed statute or for violating separation provisions criminalizing the failure to return national security information to the government.[399] Furthermore, some commentators regarded the legislation as inherently suspicious because many high-level government officials leak information as part of their "news management" efforts.[400] Critics have expressed concern that such legislation could undermine the important dialogue between government officials and the media about national security issues, and could also discourage whistleblowers and stifle public debate on important government issues.[401] Most likely such sweeping legislation would actually do little to stop unauthorized leaks by top administration officials, and would instead chill only the lower-level whistleblowing employees.[402] In addition, just because information is classified does not mean that it has been classified properly, nor does it mean that the information has been kept secret from the American public.[403]

---

[395] Papandrea, *supra* note 3, at 262-63.

[396] H.R. DOC. NO. 106-309, at 1-2 (2000).

[397] *Id.* at 1.

[398] Press Release, Sunshine in Gov't Initiative, Bond Legislation Would Create an "Official Secrets Act" and Would Shield Information from the Public About Its Government (Sept. 14, 2006), *archived at* http://perma.cc/JSF2-FK93.

[399] *See, e.g.*, Louis B. Schwartz, *Reform of Federal Criminal Laws: Issues, Tactics and Prospects*, 1977 DUKE L.J. 171, 197-99.

[400] *Id.* at 199 ("Suspicion of the 'Official Secrets Act' was further intensified by common knowledge that intentional leaks relating to vital elements of international policy and security are a common feature of 'news management' by the highest executive officers.").

[401] *See, e.g.*, Press Release, Sunshine in Gov't Initiative, *supra* note 398.

[402] Letter from John Ashcroft, U.S. Attorney Gen., to Honorable J. Dennis Hastert, Speaker of the U.S. House of Representatives (Oct. 20, 2002), *archived at* http://perma.cc/YUL6-YN8V ("The extent to which such a provision would yield any practical additional benefits to the government in terms of improving our ability to identify those who engage in unauthorized disclosures of classified information or deterring such activity is unclear, however.").

[403] *See* Fiona Morgan, *The Case for Leaks*, SALON (Nov. 1, 2000, 9:16 PM), http://www.

Despite the repeated defeat of proposals to adopt the equivalent of an "Official Secrets Act" here in the United States, the existing criminal statutes give DOJ sufficient means for prosecuting unauthorized leaks. Indeed, government officials testifying before Congress have repeatedly said that the problem with prosecuting leakers does not lie in a lack of criminal statutes penalizing the disclosure of national security information.[404] Although the name of the Espionage Act might suggest that it is limited to spies, the plain language of the statute and its legislative history reveal that it is not so limited.[405]

Classic espionage is covered in 18 U.S.C. § 794(a)-(b). Section 794(a) prohibits the transmission of documents or information relating to the national defense to "any foreign government, or to any faction or party or military or naval force within a foreign country, whether recognized or unrecognized by the United States, or to any representative . . . thereof," provided that the defendant acted "with intent or reason to believe that it is to be used to the injury of the United States or to the advantage of a foreign nation."[406] Section 794(b), applicable only in times of war and to a limited set of disclosures, also covers what is typically regarded as espionage, though direct contact with a foreign entity or its agent is not required.[407] It applies to anyone who, "with intent that the same shall be communicated to the enemy, collects, records, publishes, or communicates, or attempts to elicit any information" regarding military operations or defenses.[408] Violators of § 794(a) and (b) can be sentenced to life in prison or even death.[409] The government has not indicted any leakers under § 794.

Leakers are commonly charged under § 793(d) of the Espionage Act, which applies to those with authorized possession of national security information. This provision prohibits the "willful" communication of national security documents and information "to any person not entitled to receive it" – which most scholars have interpreted to include the press.[410] There is some debate about the scienter requirements for this statute. In criminal law, "willful" intent simply requires that the defendant act with knowledge that his conduct was unlawful; this requirement is met in most leak cases. Another portion of the statute, however, requires that the defendant had "reason to believe [the

salon.com/2000/11/02/security_3, *archived at* http://perma.cc/X36T-HKD9.

[404] *See, e.g.*, Letter from John Ashcroft to J. Dennis Hastert, *supra* note 402, at 3.

[405] *See* United States v. Morison, 844 F.2d 1057, 1063-64 (4th Cir. 1988).

[406] 18 U.S.C. § 794(a) (2012).

[407] *Id.* § 794(b).

[408] *Id.*

[409] *Id.* § 794(a)-(b) (providing that violations under either of these sections "shall be punished by death or by imprisonment for any term of years or for life").

[410] *See, e.g.*, *Morison*, 844 F.2d at 1064-70 (concluding that § 793(d) applies to disclosures to the press). *Morison* relied on the classification system in its holding that this requirement was not unconstitutionally vague. *Id.* at 1075.

disclosed information] could be used to the injury of the United States or to the advantage of any foreign nation."[411] There is some debate whether this provision modifies only "information," which precedes the phrase, or all the documents listed earlier in the statute.[412] The Act does not require that the disclosure harm the nation; it can be sufficient if the disclosure potentially benefits a foreign nation, whether friend or foe.[413] The leaker's intent to contribute to the public debate is irrelevant.[414] The statute provides for a punishment of a fine and/or ten years of imprisonment.[415]

The Supreme Court has recognized that the term "national defense" in the context of the Espionage Act statutes "is a generic concept of broad connotations, referring to the military and naval establishments and the related activities of national preparedness."[416] Most courts interpreting §§ 793 and 794 – both of which prohibit the disclosure of "information relating to the national defense" – have limited the sections' applicability to information that was closely held and whose disclosure was "potentially damaging to the United States or might be useful to the enemy."[417] A recent district court decision relying on the plain language of the statute held that even this minimal showing was not required.[418] Those courts that have required a showing of

[411] 18 U.S.C. § 793(d).

[412] *See* United States v. Rosen, 445 F. Supp. 2d 602, 625-27 (E.D. Va. 2006), *aff'd*, 557 F.3d 192 (4th Cir. 2009) (rejecting vagueness and duplicity arguments pertaining to the requirement that the defendant had "reason to believe [the disclosed information] could be used to the injury of the United States or to the advantage of any foreign nation," because the requirement pertains specifically to "intangible" information in a qualitative sense, compared to the physical or tangible nature of the information itself (internal quotation marks omitted)).

[413] *See Morison*, 844 F.2d at 1071-74 (holding that because "the defendant . . . knew that he was dealing with national defense materials" potentially advantageous to foreign governments, the scienter requirement of willfulness was met).

[414] *Id.* at 1063 (affirming the conviction of a defendant who provided stolen classified information about explosions in Russia and intelligence photographs to a publication from which he was seeking full-time employment because "[t]he language of the . . . statute[] declare[s] no exemption in favor of one who leaks to the press").

[415] 18 U.S.C. § 793 ("Whoever [violates a provision of this title] [s]hall be fined under this title or imprisoned not more than ten years, or both."); *id.* § 3571.

[416] Gorin v. United States, 312 U.S. 19, 28 (1941).

[417] *See, e.g.*, *Rosen*, 445 F. Supp. 2d at 621 ("The second judicially imposed limitation on the phrase 'information relating to the national defense' is the requirement that its 'disclosure would be potentially damaging to the United States or useful to an enemy of the United States.'" (quoting *Morison*, 844 F.2d at 1071-72)).

[418] Memorandum Opinion Granting in Part Defendant's Third Motion to Compel at 9-10, United States v. Kim, Criminal No. 10-255 (CKK) (D.D.C. May 30, 2013), *archived at* http ://perma.cc/9EJ4-PM7K ("[T]he Court declines to construe section 793(d) to require the Government to show that the disclosure of the information would be potentially damaging to the United States or might be useful to an enemy of the United States in order to satisfy the statutory requirement that the information relate to the 'national defense.'").

potential harm have explained that "[t]his important requirement is implicit in the purpose of the statute and assures that the government cannot abuse the statute by penalizing citizens for discussing information the government has no compelling reason to keep confidential."[419] Classification is neither required nor sufficient to support the prosecution's showing that the revealed information was potentially damaging.[420]

Other provisions of the Espionage Act restrict the disclosure of more specific categories of information. For example, § 798 bans the dissemination of "classified information . . . concerning the communication intelligence activities of the United States."[421] This statute does not require any showing of harm or "intent or reason to believe" any such harm or benefit to a foreign power would result. The Atomic Energy Act permits government insiders to be prosecuted for communicating "Restricted Data" to anyone not authorized to receive it, as long as they did so "knowing or having reason to believe" that the information was restricted data.[422] Former CIA operative John Kiriakou pleaded guilty to violating the Intelligence Identities Protection Act,[423] which prohibits someone with authorized access to classified information identifying a covert agent from intentionally revealing that information to anyone not entitled to receive it.[424] Leakers have also been charged under 18 U.S.C. § 641, which imposes criminal liability for the theft, conveyance, or sale of government property.[425] This provision also does not require any showing of harm to the United States or any consideration of the public interest.[426] In 2002, a government employee pled guilty to charges under this statute after he sold confidential but unclassified information to a London newspaper.[427] The government has also charged government insiders under this law – including Daniel Ellsberg – even when they have not received any pecuniary benefits.[428] Another useful provision for leak prosecutions is the Computer Fraud and

[419] *Rosen*, 445 F. Supp. 2d at 621.

[420] *See, e.g.*, *id.* at 623.

[421] 18 U.S.C. § 798(a) (2012).

[422] 42 U.S.C. § 2277 (2006). "Restricted Data" is statutorily defined as "all data concerning (1) design, manufacture, or utilization of atomic weapons; (2) the production of special nuclear material; or (3) the use of special nuclear material in the production of energy." *Id.* § 2014(y).

[423] Charlie Savage, *Former CIA Operative Pleads Guilty in Leak of Colleague's Name*, N.Y. TIMES, Oct. 23, 2012, at A16.

[424] 50 U.S.C. § 421(a)-(b) (2006).

[425] 18 U.S.C. § 641 (2012).

[426] *See id.* § 641; *see also* United States v. Morison, 844 F.2d 1057, 1076-77 (4th Cir. 1988).

[427] Ashcroft v. Randel, 391 F. Supp. 2d 1214, 1218 (2005); Rebecca Daugherty & Gil Shochat, *DEA Analyst Given One-Year Jail Sentence for Leaking Unclassified Information*, NEWS MEDIA & L., Winter 2003, at 25.

[428] Melville Nimmer, *National Security Secrets v. Free Speech: The Issues Left Undecided in the Ellsberg Case*, 26 STAN. L. REV. 311, 315-24 (1974).

Abuse Act, the broadest provision of which punishes whoever "intentionally . . . exceeds authorized access, and thereby obtains . . . information from any protected computer."[429]

The government has also used other criminal law provisions against government insiders who disclosed national security information without authorization. Some of these charges are based on the mishandling of sensitive government information. Another possibility is to charge the government insider with obstruction of justice,[430] perjury,[431] or the making of false statements[432] during a leak investigation. These statutes are available even if it is ultimately determined that no underlying criminal activity took place. The prosecution and conviction of Scooter Libby is a high-profile example of a case in which the government relied on § 1001.[433] In that case, the government ultimately decided not to pursue charges under the Intelligence Identities Protection Act because it could not prove all of the elements of that crime.[434]

III. INTELLIGENCE COMMUNITY INSIDERS AND THE FIRST AMENDMENT

Commentators have generally assumed that the First Amendment offers no protection to government insiders who engage in the unauthorized disclosure of national security information. Although the Supreme Court has never decided whether government insiders have a First Amendment right to disclose national security information without authorization, its decisions conceptually related to that issue are admittedly not promising. In addition, the only appellate court decision to address whether leakers have First Amendment rights ruled against the leaker.[435] Courts are generally reluctant to interfere with the national security decisions of the executive branch, including its methods of controlling the flow of information to the public.[436]

The Supreme Court has stated that government employees do not enjoy the same First Amendment rights as ordinary citizens.[437] Although the Court has rejected the traditional view that the government can condition the benefit of public employment on the relinquishment of First Amendment rights, the Court's jurisprudence in this area has become increasingly less protective of employee speech rights in recent years.[438]

---

[429] 18 U.S.C. § 1030(a)(2)(C).

[430] *Id.* § 1503.

[431] *Id.* § 1623.

[432] *Id.* § 1001(a)(2).

[433] Anthony S. Barkow & Beth George, *Prosecuting Political Defendants*, 44 GA. L. REV. 953, 957-65 (2010).

[434] *Id.* at 961.

[435] United States v. Morison, 844 F.2d 1057, 1068, 1080 (4th Cir. 1988).

[436] William Lee, *Left out in the Cold? The Chilling of Speech, Association, and the Press in Post-9/11 America*, 57 AM. U. L. REV. 1453, 1461 (2007).

[437] United States v. Aguilar, 515 U.S. 593, 606 (1992).

[438] *See* Garcetti v. Ceballos, 547 U.S. 410, 423-24 (2006).

This Part takes on the various arguments that the First Amendment offers no protection to intelligence community insiders who disclose national security information. It begins by rebutting the argument that the unauthorized dissemination of national security information is not even "speech" under the First Amendment and goes on to tackle the claim that the First Amendment does not protect those "entrusted" with information. Next, this tackles the common argument that government insiders waive their First Amendment rights when they sign nondisclosure contracts. After concluding that laws restricting the unauthorized disclosures of national security information are subject to First Amendment analysis, this Part discusses the Court's jurisprudence regarding national security insiders as well as the rights of government employees more generally. It concludes that the Court's jurisprudence does not entirely foreclose the First Amendment claims of national security insiders. Instead, any restriction on their expressive activities is subject to constitutional scrutiny with due consideration given to the value of the speech and the resulting harm.[439]

A. *Most Leaks Are "Speech"*

The government has repeatedly argued that the dissemination of national security information is not speech protected under the First Amendment. It has made this this argument with respect to both government insiders and outsiders. This argument has had mixed success in the lower courts.[440] The answer to this question is crucial, because if the speech is not entitled to any

[439] William Van Alstyne, *A Graphic Review of the Free Speech Clause*, 70 CALIF. L. REV. 107, 114 (1982) (stating that lying on the witness stand might be perjury, but it is still speech); Eugene Volokh, *Speech as Conduct: Generally Applicable Laws, Illegal Courses of Conduct, "Situation-Altering Utterances," and the Uncharted Zones*, 90 CORNELL L. REV. 1277, 1339 (2005) (arguing that certain types of speech ought to be punished under a "crime-facilitating" speech exception to First Amendment protection, and that "courts should develop the boundaries [of this exception] by considering the usual First Amendment factors – the value of the speech, the harm that it causes, the difficulty of drawing certain lines, the risk that punishing some speech will deter other speech, and so on" (citation omitted)).

[440] *Compare* United States v. Kim, No. 10-225, 2011 WL 838160, at *30 (D.D.C. Mar. 2, 2011) ("To the extent that the defendant's conduct constitutes speech, that speech is wholly unprotected by the First Amendment."), *with* United States v. Rosen, 445 F. Supp. 2d 602, 629-30 (E.D. Va. 2006) (rejecting the Government's categorical argument that the espionage statutes do not implicate the First Amendment), *aff'd*, 557 F.3d 192 (4th Cir. 2009). In *United States v. Morison*, the panel opinion stated "we do not perceive any First Amendment rights to be implicated here." *Morison*, 844 F.2d at 1068. Two of the three judges, however, indicated in their concurring opinions that they simply believed that the conviction in that particular case did not offend the First Amendment. *See id.* at 1081 (Wilkinson, J., concurring); *id.* at 1085 (Phillips, J., concurring).

First Amendment protection, judicial review is at an end, and the government is generally able to restrict that speech as it wishes.[441]

The government and commentators have made several arguments why the unauthorized disclosure of national security information falls outside of the First Amendment: (1) unauthorized disclosures of national security information are not speech; (2) government insiders have been entrusted with the information and have obligations not to reveal it; (3) relatedly, government insiders have contractually waived any First Amendment rights they may have possessed; and (4) *Garcetti v. Cebellos* eliminated First Amendment protection for the disclosure of any information obtained on the job. This Section dissects each of these arguments.

1. Unauthorized Disclosures Are Speech

As Frederick Schauer has observed, "questions about the involvement of the First Amendment in the first instance are often far more consequential than are issues surrounding the strength of protection that the First Amendment affords to the speech to which it applies."[442] Determining whether something that is clearly "speech" falls within the scope of the First Amendment remains an unresolved and hotly debated issue, even outside of the national security context. The Court has held that certain categories of speech – like incitement, obscenity, child pornography, commercial speech, defamation, fighting words, and true threats – are "speech" within the meaning of the First Amendment but receive no protection.[443] In the last several decades, the Court has revisited some of these categories and held that the First Amendment does in fact provide some protection. Commercial speech[444] and defamation[445] are the two most obvious examples of this. It is unclear whether "fighting words" is still a viable category of unprotected speech.[446] The Court has added child pornography[447] and true threats[448] as categories of unprotected speech, but it has rejected the government's efforts, in the context of "crush" animal videos, violent video games, and autobiographical lies, to add additional categories based merely on a balancing of the harm and the value of the speech.[449]

---

[441] *But see* R.A.V. v. City of St. Paul, 505 U.S. 377, 388 (1992) (holding that the government cannot make content-based distinctions within a category of unprotected speech unless that distinction rests on the reason the category exists).

[442] Frederick Schauer, *The Boundaries of the First Amendment: A Preliminary Exploration of Constitutional Salience*, 117 HARV. L. REV. 1765, 1767 (2004).

[443] United States v. Alvarez, 132 S. Ct. 2537, 2544 (2012).

[444] Va. State Bd. Pharmacy v. Va. Consumer Council, Inc., 425 U.S. 748 (1976).

[445] N.Y. Times Co. v. Sullivan, 376 U.S. 254 (1964).

[446] Schauer, *supra* note 442, at 1777 & n.53.

[447] New York v. Ferber, 458 U.S. 747 (1982).

[448] Virginia v. Black, 538 U.S. 343 (2003).

[449] Brown v. Entm't Merchs. Ass'n, 123 S. Ct. 2729, 2742 (2011) (rejecting the argument that violent video games were not "speech"); United States v. Stevens, 130 S. Ct.

But the Court has failed to recognize First Amendment protection in a wide variety of other contexts. Sometimes the Court is explicit. The best example comes in the copyright context, where the Court has rejected First Amendment challenges to copyright law.[450] In other cases, the Court simply does not address potential First Amendment defenses,[451] or only lower courts have addressed whether the First Amendment is applicable. Examples include securities regulation,[452] as well as antitrust, panhandling, hostile-environment sexual harassment, computer source code, conspiracy, criminal solicitation, fraud, trademark, and rules of evidence.[453] It is important to note that in these contexts, it is not that the Court has determined that the speech restriction at issue satisfies some level of scrutiny; instead, the government's actions are simply not subject to any First Amendment analysis at all. In other words, at least with speech that arguably constitutes incitement, for example, the government must demonstrate that the relevant law satisfies the *Brandenburg* test for incitement. In the context of conspiracy, the Court does not apply even that lesser level of First Amendment scrutiny.[454]

One reason why it is so difficult to tell what the First Amendment covers is that the word "speech" is a broad term that covers much of what we do in our everyday lives.[455] As Justice Holmes once said, "the First Amendment, while prohibiting legislation against free speech as such cannot have been, and obviously was not, intended to give immunity for every possible use of language."[456] The Court has never held that "the presence of 'words' [is] a

1577, 1585 (2010) (rejecting arguments that "crush" videos were not speech); United States v. Alvarez, 132 S. Ct. 2537, 2544 (2012) (rejecting the argument that lies are not speech).

[450] *See, e.g.*, Eldred v. Ashcroft, 537 U.S. 186, 221 (2003) (dismissing First Amendment objections to the Copyright Term Extension Act); Harper & Row Publishers, Inc. v. Nat'l Enters., 471 U.S. 539, 555-60 (1985) (holding that the First Amendment does not require a public figure exception to the fair use doctrine); Margot Kaminski, *Copyright Crime and Punishment: The First Amendment's Proportionality Problem*, 73 MD. L. REV. (forthcoming 2014) (arguing for the consideration of First Amendment concerns through a proportionality approach to copyright law); Mark A. Lemley & Eugene Volokh, *Freedom of Speech and Injunctions in Intellectual Property Cases*, 48 DUKE L.J. 147, 169-80 (1998) (arguing for an extension of prior restraint principles to intellectual property cases); Neil Weinstock Netanel, *Locating Copyright Within the First Amendment Skein*, 54 STAN. L. REV. 1, 4-5 (2001) (arguing for First Amendment scrutiny of copyright law).

[451] *See, e.g.*, Harris v. Forklift Sys., Inc., 510 U.S. 17 (1993) (failing to mention a First Amendment objection to a Title VII action even though the argument had been raised in the briefs); R.A.V. v. City of St. Paul, 505 U.S. 377, 389-90 (1992) (rejecting a First Amendment defense to a Title VII action in dicta).

[452] *See* Symposium, *The First Amendment and Federal Securities Regulation*, 20 CONN. L. REV. 261 (1988).

[453] Schauer, *supra* note 442, at 1766-77 & n.7, 1783-84.

[454] *Id.* at 1769-71.

[455] *Id.* at 1773.

[456] Frohwerk v. United States, 249 U.S. 204, 206 (1919).

'sufficient condition' for testing the regulation of [speech] against First Amendment standards."[457]

Robert Post has argued that "First Amendment analysis is relevant only when the values served by the First Amendment are implicated."[458] Unfortunately, the Court has not consistently embraced a particular theory of the First Amendment. Several different theories for First Amendment protection exist, including the marketplace of ideas, self-governance, autonomy, toleration, distrust of government, checking government abuse, and perhaps others. No single theory, however, can explain the Court's existing jurisprudence. Because these various theories apply in some cases and not others, it is hard to use any of these theories to determine definitively what speech is "in" and what speech is "out."[459]

Despite the uncertainty regarding how to determine what counts as "speech" for First Amendment purposes, it is possible that the speech involved in traditional espionage is not speech that the First Amendment protects.[460] If one analyzes the various theories supporting the protection of speech under the First Amendment, it is hard to see how espionage fits in. Traditional espionage involves the secret exchange of information; accordingly, by definition, it does not contribute to the marketplace of ideas and cannot be said to promote self-government and deliberation.[461] Although the Court has been reluctant to create new categories of unprotected expression,[462] it is quite possible that espionage has a sufficient historical pedigree to justify the Court's recognition of espionage as unprotected speech.

Even if espionage is a category of unprotected expression, however, a precise definition of that category is essential. Not all speech secretly communicated to a foreign power or hostile entity is espionage, particularly if it is information already in the public domain.[463] Furthermore, as one federal court of appeals has recognized, not all national security information communicated to a foreign power or hostile entity poses harm to the national security interests of the United States.[464] In addition, one hallmark of

[457] Schauer, *supra* note 442, at 1777.

[458] Robert Post, *Recuperating First Amendment Doctrine*, 47 STAN. L. REV. 1249, 1255 (1995).

[459] Schauer, *supra* note 442, at 1784-87.

[460] United States v. Rosenberg, 195 F.2d 583, 591 (2d Cir. 1952) ("The communication to a foreign government of secret material connected with the national defense can by no far-fetched reasoning be included within the area of First-Amendment protected free speech.").

[461] *See* Thomas Emerson, *National Security and Civil Liberties*, 9 YALE J. WORLD PUB. ORD. 78, 87-88 (1982).

[462] *See, e.g.*, United States v. Stevens, 559 U.S. 460, 468-72 (2010) (refusing to recognize "depictions of animal cruelty" as a category of unprotected speech).

[463] *See* Gorin v. United States, 32 U.S. 19 (1941) (holding that the Espionage Act did not apply to information that the military had made public).

[464] United States v. Heine, 151 F.2d 813, 815-17 (2d Cir. 1945) (expressing concern that

espionage is that the information is disseminated with the intent of reaching the foreign power rather than the American public.[465]

National security information is generally core political speech, and like other kinds of political speech, it can make a valuable contribution to the public debate.[466] National security information is a category that is virtually without limits and hard to distinguish from information pertaining to the general welfare.[467] Certainly the fact that some government official has classified a document as "secret" should not end all First Amendment inquiry and render the courts "powerless to go beyond such legislative or administrative action."[468]

As Thomas Emerson has argued, "the existence of a national security interest does not in and of itself justify alteration of constitutional principles, but is merely one factor in the application of constitutional principle."[469] Instead, "the focus turns not toward a general definition of national security but toward an examination of the specific national security factors involved in the particular situation."[470] Indeed, the Pentagon Papers case indicates that the government's attempts to control the dissemination of national security information are subject to First Amendment analysis.[471] Although that case involved a prior restraint and not subsequent criminal punishment, even the dissenting Justices who argued for a sharply limited judicial role regarding the executive's national security decisions did not argue that restrictions on the dissemination of national security information are immune from First Amendment scrutiny.

---

statutes prohibiting the disclosure of information "advantageous to a foreign nation," even if not harmful to the United States, sweep too broadly, stating, "so drastic a repression of the free exchange of any information it is wise carefully to scrutinize, lest extravagant and absurd consequences result").

[465] Professor Emerson has argued that essential to any definition of espionage as a category of unprotected expression is also a requirement that "the government prove that the person making the communication has done so with the primary intent that the information be used by the foreign power to the injury of our national defense." Emerson, *supra* note 461, at 88. As discussed in Part II, requiring some sort of intent that the information would be used to injure our national defense might narrow the definition of espionage.

[466] *Compare* Bruce Methven, Comment, *First Amendment Standards for Subsequent Punishment of Dissemination of Confidential Government Information*, 68 CALIF. L. REV. 83, 86-87 (1980) (arguing that there is a distinction between "pure political speech," which is entitled to robust First Amendment protection, and leaks of national security information, which are entitled to some lesser amount of protection).

[467] *See* Emerson, *supra* note 461, at 78-79 (discussing broad and narrow conceptions of national security).

[468] Nimmer, *supra* note 428, at 328.

[469] Emerson, *supra* note 461, at 79.

[470] *Id.*

[471] N.Y. Times Co. v. United States, 403 U.S. 713, 714 (1971).

2. Professional Duty

The government's argument that the unauthorized dissemination of national security information falls completely outside of the First Amendment has little merit. Much weightier is the government's argument that the First Amendment does not apply to government insiders because they have been entrusted with that information and have a professional obligation not to disclose it.[472]

In support of its argument, the government often relies on language in various appellate and Supreme Court decisions stating that one who is entrusted with information has no First Amendment right to disseminate it. One frequently cited[473] case is *United States v. Aguilar*,[474] where the Supreme Court upheld the conviction of a federal judge who revealed the contents of a wiretapping application[475] based on the principle that "those who accept positions of trust involving a duty not to disclose information they lawfully acquire while performing their responsibilities have no First Amendment right to disclose that information."[476]

A closer reading of *Aguilar* reveals, however, that the judge in that case was not convicted simply of passing along information about a wiretap, but rather was convicted under a specific statute applicable only when someone gives notice or attempts to give notice about an authorized wiretap warrant "in order to obstruct, impede, or prevent [the] interception."[477] In other words, this statute requires that someone have the specific intent to interfere with an authorized wiretap – it does not impose a general duty of nondisclosure.[478] Furthermore, it is not hard to see how such a statute would satisfy strict scrutiny; indeed, *Aguilar* concluded that "the Government's interest is quite sufficient to justify the construction of the statute as written, without any artificial narrowing because of First Amendment concerns."[479]

To be sure, *Aguilar*'s constitutional analysis is not the model of clarity. The majority opinion also states without qualification that "[g]overnment officials

---

[472] *See, e.g.*, Lee, *supra* note 4, at 1461 (concluding that government insiders' duty of nondisclosure prevents courts from recognizing the First Amendment rights of leakers); Edward Xanders, *A Handyman's Guide to Fixing National Security Leaks: An Analytical Framework for Evaluating Proposals to Curb Unauthorized Publication of Classified Information*, 5 J.L. & POL. 759, 800 (1989) (arguing that it is "morally justifiable" to require government employees to keep secrets "in light of the special nature of their positions").

[473] *See, e.g.*, United States v. Kim, 808 F. Supp. 2d 44, 57 (D.D.C. 2011); Wilson v. CIA, 586 F.3d 171, 183 (2d Cir. 2009).

[474] 515 U.S. 593 (1995).

[475] *Id.*

[476] Boehner v. McDermott, 484 F.3d 573, 579 (D.C. Cir. 2007) (en banc).

[477] 18 U.S.C. § 2232(d) (2012).

[478] *Aguilar*, 515 U.S. at 603; *see also Boehner*, 484 F.3d at 588-90 (Sentelle, J., dissenting) (noting the limits of *Aguilar*).

[479] *Aguilar*, 515 U.S. at 606.

in sensitive confidential positions may have special duties of nondisclosure."[480] To support this point, the Court cites Federal Rule of Criminal Procedure 6(e),[481] which prohibits the disclosure of grand jury information, and *Seattle Times v. Rhinehart*,[482] which upheld the imposition of protective orders preventing attorneys from disseminating information obtained during civil discovery.[483] The Court could have also cited *Cohen v. Cowles*, which upheld the breach of contract claim of a source whose identity was revealed.[484] Indeed, the D.C. Circuit relied on the foregoing cases in *Boehner v. McDermott*, where it stated categorically that "those who accept positions of trust involving a duty not to disclose information they lawfully acquire while performing their responsibilities have no First Amendment right to disclose that information."[485] But none of these cases rests on the categorical assumption that the speech at issue was not "speech" within the meaning of the First Amendment; instead, the holdings were limited to the particular claims at issue in those cases.[486]

The Court's recent decision in *United States v. Alvarez*[487] supports the argument that determining whether speech falls outside the protections of the First Amendment is a highly context-specific inquiry.[488] The Court recognized that some false speech – like perjury – is not protected under the First Amendment, but rejected the government's argument that it therefore followed that all false speech was outside of the First Amendment.[489] Instead, certain false statements are unprotected because of the context in which they occur.[490] In his concurrence, Justice Breyer also emphasized the importance of context in distinguishing between protected and unprotected speech.[491] The same can be said with regard to the dissemination of national security information. First Amendment protection depends on what, to whom, and why information is disclosed.

[480] *Id.*

[481] *Id.*

[482] 467 U.S. 20, 31 (1984).

[483] *Aguilar*, 515 U.S. at 606.

[484] Cohen v. Cowles Media Co., 501 U.S. 663, 672 (1991).

[485] Boehner v. McDermott, 484 F.3d 573, 579 (D.C. Cir. 2007) (en banc).

[486] *See id.* at 588 (Sentelle, J., dissenting).

[487] 132 S. Ct. 2537 (2012).

[488] *Id.* at 2539-40 (plurality opinion).

[489] *Id.* at 2545-46.

[490] *Id.* at 2546 (explaining that the fact that certain types of falsehoods are unprotected "does not lead to the broader proposition that false statements are unprotected when made to any person, at any time, in any context").

[491] *Id.* at 2553-54 (Breyer, J., concurring).

3. Limits of Contractual Waiver Argument

One of the biggest obstacles facing government insiders who engage in the unauthorized dissemination of national security information is that they have signed nondisclosure agreements that arguably amount to a waiver of rights they might have otherwise enjoyed to disclose information. Although the trust relationship between the government and its employees does support some restrictions on the dissemination of information obtained as a result of that relationship, it is essential to recognize that "contracts are not enforced simply because they are made."[492] As a matter of contract law, confidentiality agreements cannot be enforced when they violate public policy.[493] As a result, the existence of these contracts should not be regarded as an absolute bar to any First Amendment claim a government insider might make.

Since 1983, all government employees and contractors with access to national security information have been required to sign nondisclosure agreements.[494] These agreements provide that the government insider will not disclose classified information to anyone unauthorized to receive it and will submit to the government for prepublication review any communications they plan to make to the public, including speeches, articles, and books, including works of fiction.[495] The purpose of requiring employees to sign confidentiality contracts is to promote employee awareness of their duty to keep information secret and to reduce the chances of inadvertent disclosure.[496] Before obtaining access to classified information, government employees are also required to receive training on "basic security policies, principles, practices, and criminal, civil, and administrative penalties."[497]

The government is not alone in requiring its employees to sign nondisclosure agreements. Indeed, such agreements are very common in the private sector and are used for a variety of reasons.[498] On their face, these agreements apply regardless of the purpose for which an unauthorized disclosure is made.[499] In most cases, confidentiality agreements serve the public interest, as they prevent the disclosure of sensitive private, financial, or government information, protect valuable trade secrets, encourage the sharing

[492] Medow, *supra* note 4, at 811-12.

[493] Perricone v. Perricone, 972 A.2d 666, 685 (Conn. 2009).

[494] National Security Decision Directive 84 (1983), *archived at* http://perma.cc/8JAS-V5XS.

[495] Dep't of Def., Form 1847-1, Sensitive Compartmented Information Nondisclosure Statement (1991) (illustrating the terms of an agreement that government employees sign regarding their access to confidential government information).

[496] Timothy Morehead Dworkin & Elletta Sangrey Callahan, *Buying Silence*, 36 AM. BUS. L.J. 151, 157 (1998).

[497] 32 C.F.R. § 2001.71(b) (2013).

[498] *See* Garfield, *supra* note 15, at 268-74.

[499] *Id.* at 302-03 (explaining that the law rejects arguments that contend that the protection of trade secrets harms public and commercial interests).

of information, and in the case of settlement agreements, promote dispute resolution.[500] In some instances, however, nondisclosure agreements can suppress the sharing of newsworthy information about public health and safety as well as the conduct of important public figures and public officials.[501] It would be a mistake to declare, as did the trial court in *Cohen v. Cowles Media Co.*, that "[t]his is not a case about free speech, rather it is one about contracts."[502]

The enforceability of confidentiality agreements received significant scholarly attention in the 1990s after Jeffrey Wigand, a former vice president for research and development at Brown & Williamson Tobacco Corp., revealed that top executives had knowingly approved the use of addictive additives in their products.[503] Right before *60 Minutes* was about to air an interview with whistleblower Wigand, CBS withdrew the segment because the tobacco company had threatened to sue the station for tortious interference with a contract.[504] Soon thereafter, confidentiality agreements were under attack in a number of other high-profile cases. For example, in 1996, the Equal Employment Opportunity Commission (EEOC) successfully voided a company's settlement agreements with current and former employees on grounds that the agreements undermined the Commission's ability to conduct investigations, two of which involved allegations of class-wide sexual harassment.[505]

Confidentiality agreements are not automatically enforceable. Although the precise inquiry can vary from state to state, many states permit the enforceability of confidentiality agreements only when they are "reasonable."[506] One factor that states frequently consider as part of the "reasonableness" inquiry is whether the agreements are more restrictive than necessary.[507] For example, courts have routinely held that nondisclosure agreements are unenforceable when they preclude the use of information

[500] *Id.* at 275.

[501] *Id.*

[502] 14 Med. L. Rep. 1460, 1464 (Minn. Dist. Ct. 1987).

[503] *See, e.g.*, Dworkin & Callahan, *supra* note 496, at 151-52; Garfield, *supra* note 15, at 264-65; Brian Stryker Weinstein, *In Defense of Jeffrey Wigand: A First Amendment Challenge to the Enforcement of Employee Confidentiality Agreements*, 49 S.C. L. REV. 129, 131 (1997). Some scholars have argued that in such circumstances, the contracts are unenforceable either because they violate public policy or because they violate the First Amendment (or both). *See, e.g.*, Carol M. Bast, *At What Price Silence: Are Confidentiality Agreements Enforceable?*, 25 WM. MITCHELL L. REV. 627, 707-08 (1999) (arguing in favor of a public policy exception to confidentiality agreements); Weinstein, *supra* (arguing for First Amendment protection for whistleblowers).

[504] Marie Brenner, *The Man Who Knew Too Much*, VANITY FAIR, May 1996, at 170.

[505] *See* EEOC v. Astra U.S.A., 929 F. Supp. 512 (D. Mass. 1996), *modified*, 94 F.3d 738 (1st Cir. 1996).

[506] Bast, *supra* note 503, at 639-44.

[507] *Id.*

already publically available.[508] These cases typically arise in the context of trade secret litigation when a court denies enforcement of a contract because the information at issue does not qualify as a trade secret.[509] In the national security arena, the analogous situation would arise if the government tried to enforce a contract to protect information that is not closely held. The contract might also be unenforceable if the information does not pose any harm to national security.[510]

Another method of attacking the validity of a nondisclosure agreement is to argue that its enforcement is against public policy. The *Restatement (Second) of Contracts* section 178(1) provides that a contract is "unenforceable on grounds of public policy if legislation provides that it is unenforceable or the interest in its enforcement is clearly outweighed in the circumstances by a public policy against the enforcement."[511] Under this balancing approach, the scope of the public policy exception is unclear; it can also lead to varied results over time as community mores change.[512] Although courts sometimes express reservations about the public policy exception "of indefinite and uncertain definition,"[513] they nevertheless have frequently refused to enforce a wide variety of contracts on public policy grounds based on their own view of right and wrong.[514]

Analogizing national security secrets to trade secrets does not support the argument that the government has unlimited power to punish government insiders. Trade secret law is also subject to exceptions for the public interest. The Uniform Trade Secrets Act recognizes that "exceptional circumstances" may protect the disclosure of trade secrets despite the potential harm to the

[508] *See, e.g.*, Nasco, Inc. v. Gimbert, 238 S.E.2d 368, 369-70 (Ga. 1977) ("This nondisclosure covenant is overly broad and unreasonable in that it would prohibit disclosure of information not needed for the protection of the employer's legitimate business interests."); Cherne Indus. v. Grounds & Assoc., 278 N.W.2d 81, 90 (Minn. 1979) ("[M]atters of general knowledge within the industry may not be classified as trade secrets or confidential information entitled to protection." (quoting Whitmyer Bros. v. Doyle, 274 A.2d 577, 581 (N.J. 1971) (internal quotation marks omitted)).

[509] *See, e.g.*, *Cherne*, 278 N.W.2d at 90; *Nasco*, 238 S.E.2d at 369-70.

[510] *See, e.g.*, Ctr. for Int'l Envtl. Law v. Office of U.S. Trade Representative, 845 F. Supp. 2d 252, 256 (D.D.C. 2012), *rev'd*, 718 F.3d 899 (D.C. Cir. 2013).

[511] RESTATEMENT (SECOND) OF CONTRACTS § 178(1) (1981).

[512] Garfield, *supra* note 15, at 294, 298; *see also* Richardson v. Mellish, (1824) 130 Eng. Rep. 294 (C.P.); 2 Bing. 229 (describing the public policy exception as "a very unruly horse, and when once you get astride it you never know where it will carry you").

[513] *In re* Marriage of Witten, 672 N.W.2d 768, 779 (Iowa 2003).

[514] *See, e.g.*, Verduzco v. Gen. Dynamics, 742 F. Supp. 559, 560-61 (S.D. Cal. 1990) (applying a public policy exception "not based on or derived from a statute" in a case in which an employee reported to his defense contractor employer that security was so lax it compromised national security, and citing "general societal concerns" for the health, safety, and welfare of its citizens); 5 SAMUEL WILLISTON, A TREATISE ON THE LAW OF CONTRACTS §§ 12.2-.3 (4th ed. 2009).

trade secret owner; these "exceptional circumstances include the existence of an overriding public interest."[515] Trade secret law also recognizes a privilege to disclose trade secrets "in connection with disclosure of information that is relevant to public health or safety, or to the commission of a crime or tort, or to other matters of substantial public concern."[516] If a company claimed that the use of a certain chemical to manufacture a product was a trade secret, but that chemical was toxic, trade secret law would not protect that information.[517]

Other areas of the law also recognize exceptions to the duty of confidentiality. Although attorneys are generally required to refrain from disclosing a client's confidences relating to the attorney's representation of that client, the American Bar Association (ABA) Model Rules of Professional Conduct permit attorneys to break that confidence in a number of circumstances.[518] One exception permits attorneys to breach a client's confidence when the lawyer "reasonably believes necessary . . . to prevent reasonably certain death or substantial bodily harm."[519] All jurisdictions have adopted some form of this exception, and some jurisdictions make these sorts of disclosures mandatory.[520] As an example of what the Model Rule encompasses, the annotations state that an attorney can tell the authorities when a client has accidentally released toxic waste into a town's water supply and there is a substantial risk those who drink the water will "contract a life-threatening or debilitating disease."[521] Another exception in ABA Model Rule 1.6 permits lawyers to make disclosures when necessary "to prevent the client from committing a crime or fraud that is reasonably certain to result in substantial injury to the financial interests or property of another,"[522] or "to prevent, mitigate or rectify" such injury when the client has used or is using the lawyer's services in furtherance of the crime or fraud.[523] These exceptions to the attorney-client privilege demonstrate that other important privileges have exceptions to the usual confidentiality requirements when necessary to serve the public interest.

The government is not entitled to condition federal employment as it pleases. The Fourth Circuit has held that "the First Amendment limits the

---

[515] UNIF. TRADE SECRETS ACT § 2(b) cmt. background (1985).

[516] RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 40 cmt. c (1993).

[517] Pamela Samuelson, *Principles for Resolving Conflicts Between Trade Secrets and the First Amendment*, 58 HASTINGS L.J. 777, 788 (2007).

[518] *See, e.g.*, MODEL RULES OF PROF'L CONDUCT R. 1.6(b) (2013).

[519] *Id.*

[520] *Id.* R. 1.6 cmt. 1-20. The precise scope of the exceptions to the attorney confidentiality rules varies widely from jurisdiction to jurisdiction. For a helpful chart setting forth these differences, see JOHN DZIENKOWSKI, PROFESSIONAL RESPONSIBILITY STANDARDS, RULES & STATUTES 108-15 (2011-12 ed.).

[521] MODEL RULES OF PROF'L CONDUCT R. 1.6(b), cmt. 6.

[522] *Id.* R. 1.6(b)(2).

[523] *Id.* R. 1.6(b)(3).

extent to which the United States, contractually or otherwise, may impose secrecy requirements upon its employees and enforce them with a system of prior censorship."[524] Indeed, the Court's decisions in the public employment area suggest the same thing. The Court has never held that a law restricting the First Amendment rights of government employees passes constitutional muster simply because those employees took their positions with full knowledge of the restrictions those laws imposed.[525] As Thomas Emerson has argued, these contracts "must be viewed in First Amendment terms, not private contract terms."[526] Whether a restriction takes the form of a contract or a statute, the government's actions must still survive constitutional scrutiny. As a result, the Court has struck down laws that required government employees to take an oath regarding their political affiliation,[527] or that forbade expressions of hostility[528] or criticism of the government's policies;[529] it has also invalidated laws that banned honoraria for expression outside of work.[530]

Certainly some restrictions on the ability of government insiders to disseminate sensitive information are important for the proper functioning of the government's national security mission. At the same time, simply stating that secrecy and loyalty are important in the context of national security does not answer the question of whether these restrictions are constitutional. Furthermore, as discussed more fully below, it is hardly clear that the government can impose criminal penalties on those who violate a condition of employment. Although, as a general matter, the government – like a private employer – has good reasons for wanting its employees to keep its secrets, the trust relationship does not justify restricting the ability of employees to reveal wrongdoing or information that poses no harm to the nation's interests.

4. First Amendment Rights of Public Employees Generally

The Supreme Court has accepted the government's argument that the ordinary rules of the First Amendment do not apply to government

[524] United States v. Marchetti, 466 F.2d 1309, 1313 (4th Cir. 1972).

[525] *See, e.g.*, United States v. Nat'l Treasury Emps. Union, 513 U.S. 454, 477 (1995); U.S. Civil Serv. Comm'n v. Nat'l Ass'n of Letter Carriers, 413 U.S. 548, 551 (1973); Keyishian v. Bd. of Regents of Univ. of State of N.Y., 385 U.S. 589, 609-10 (1966); *see also* Elrod v. Burns, 427 U.S. 347, 360 n.13 (1967) (plurality opinion).

[526] *See* Emerson, *supra* note 461, at 97.

[527] *Keyishian*, 385 U.S. at 609-10; Wiemann v. Updegraff, 344 U.S. 183, 191 (1952).

[528] Rankin v. McPherson, 483 U.S. 378, 309 (1987) (holding that the State's purported interest in discharging a federal employee who made disparaging remarks about government officials did not warrant the violation of the discharged employee's First Amendment rights).

[529] Givhan v. W. Line Consol. Sch. Dist., 439 U.S. 410, 414 (1979); Pickering v. Bd. of Educ., 391 U.S. 563, 574 (1968).

[530] *Nat'l Treasury Emps. Union*, 513 U.S. at 454.

employees.[531] For decades, courts commonly understood that the First Amendment placed no restrictions on the ability of the government to discipline its employees based on their expressive activities.[532] The basis for this understanding was a rights/privilege distinction; in other words, the argument ran, being a public employee is a privilege, not a right, and the government is free to condition the exercise of that privilege on the relinquishment of constitutional rights.[533] As Oliver Wendell Holmes famously said, "[t]he petitioner may have a constitutional right to talk politics, but he has no constitutional right to be a policeman."[534]

Over time, the Court's reliance on the rights/privilege distinction diminished, and the Court instead required any restrictions on the free speech rights of public employees to pass constitutional scrutiny.[535] In its landmark 1968 decision in *Pickering v. Board of Education*, the Supreme Court held that the First Amendment provides some protection for the free speech rights of public employees to make statements regarding matters of public concern, even when the statements involve the subject matter of their employment and are critical of their ultimate supervisors.[536] The Court recognized that the government "has interests as an employer in regulating the speech of its employees that differ significantly from those it possesses in connection with regulation of the speech of the citizenry in general."[537] At the same time, the Court observed, "free and open debate is vital to informed decision-making by the electorate," and government employees often are the ones "most likely to have informed and definite opinions" about matters of public concern relating to their employment.[538] To reconcile these competing interests, the Court set up a balancing test for determining whether the employee's constitutional rights had been violated. This test requires a "balance between 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."[539]

---

[531] *See, e.g.*, Garcetti v. Ceballos, 547 U.S. 410, 421 (2006) (holding that the First Amendment only protects speech of government employees when they are speaking as private citizens, not when they are speaking pursuant to their official duties).

[532] *See* William W. Van Alstyne, *The Demise of the Right-Privilege Distinction in Constitutional Law*, 81 HARV. L. REV. 1439, 1439-40 (1968).

[533] *Id.*

[534] McAuliffe v. Mayor of New Bedford, 29 N.E. 517, 517 (Mass. 1892).

[535] *See* Perry v. Sindermann, 408 U.S. 593, 597 (1973) (holding that it was well settled that government employment could not be denied or penalized "on a basis that infringes [the employee's] constitutionally protected interests—especially, his interest in freedom of speech").

[536] 391 U.S. 563, 569-70 (1968).

[537] *Id.* at 568.

[538] *Id.* at 571-72.

[539] *Id.* at 568.

Despite broad statements in the opinion about the valuable contributions government employees can make to debates on public issues, the Court was careful to limit its holding to the facts. The case offers little direct guidance regarding the First Amendment rights of government employees who leak national security information. Indeed, the Court may have had national security leakers in mind when it noted that "[i]t is possible to conceive of some positions in public employment in which the need for confidentiality is so great that even completely correct public statements might furnish a permissible ground for dismissal."[540]

Since *Pickering*, the Court has chipped away at the First Amendment protections government employees enjoy. Most significantly,[541] in *Garcetti v. Ceballos*, the Court held that the First Amendment offers public employees no protection when they are speaking pursuant to their "official duties."[542] It did not address what counts as speaking pursuant to official employment duties, and brushed aside Justice Souter's concerns that "one response to the Court's holding will be moves by government employers to expand stated job descriptions to include more official duties and so exclude even some currently protectable speech from First Amendment purview."[543] Justice Kennedy simply stated that the job description would not be dispositive and that, instead, courts would conduct a practical inquiry in each case to determine job duties.[544] Unsurprisingly, lower courts have struggled to determine the scope of plaintiffs' job duties.[545] Some have held that raising concerns about the workplace is an element of an employee's job duties, even if making such complaints was not expressly part of the job description.[546] First Amendment

[540] *Id.* at 570 n.3.

[541] In *Connick v. Meyers*, the Court declared that public employees have to demonstrate as a threshold matter that their speech involved "a matter of public concern." 461 U.S. 138, 146 (1983). Although there certainly could be some national security disclosures that would fail the public concern inquiry, the public concern requirement will not stand as a significant barrier in the majority of cases.

[542] Garcetti v. Ceballos, 547 U.S. 410, 421 (2006).

[543] *Id.* at 431 n.2 (Souter, J., dissenting).

[544] *Id.* at 424-25.

[545] *See, e.g.*, Scott R. Bauries & Patrick Schach, *Coloring Outside the Lines:* Garcetti v. Ceballos *in the Federal Appellate Courts*, 262 EDUC. L. REP. 357 (2011); Christine Elzer, *The "Official Duties" Puzzle: Lower Courts' Struggle with First Amendment Protection for Public Employees After* Garcetti v. Ceballos, 69 U. PITT. L. REV. 367 (2007).

[546] *See, e.g.*, Huppert v. City of Pittsburgh, 574 F.3d 696, 706-07 (9th Cir. 2009) (rejecting the First Amendment claim of a police officer because he acted within his broader duties as a law enforcement officer when he cooperated in an undisclosed manner with the FBI); Davis v. McKinney, 518 F.3d 304, 315 (5th Cir. 2008) (stating that reporting misconduct through chain of command lacks First Amendment protection under *Garcetti*); Vose v. Kliment, 506 F.3d 565, 570-72 (7th Cir. 2007) (rejecting the First Amendment claim of a police officer who was forced to resign after he reported the misconduct of other officers to his superiors).

claims brought by employees who have made statements adverse to the government in the course of performing their job duties have not fared well in the lower courts.[547]

In *Garcetti*, Justice Kennedy writes that government employees have no First Amendment rights with respect to speech "that owes its existence to a public employee's professional responsibilities."[548] Professor Stephen Vladeck relies on this language to argue that national security employees must have no First Amendment right to share confidential information because they would not have access to this information but for their employment.[549] In addition, Vladeck comments, the majority appeared willing to leave whistleblower protections to the whim of legislatures who could pass statutory protections.[550]

Vladeck's interpretation of *Garcetti* goes too far.[551] In *Garcetti*, the Court attempted to draw a line between speech "as an employee" and speech "as a citizen."[552] It would not make a lot of sense to say that a public employee speaks "as an employee" every time he says something that he learned through work. In determining what an employee's official duties are, Kennedy explained that "the proper inquiry is a practical one" that should focus on "the duties an employee actually is expected to perform."[553] The appropriate inquiry, then, is not whether an employee reveals information he obtained on the job in the course of performing his job, but whether his job duties required him to disclose information. The Supreme Court may soon decide whether Vladeck or I have the better argument on how to interpret the scope of *Garcetti*.[554]

---

[547] *See, e.g.*, Green v. Barrett, 226 Fed. App'x 883, 886 (11th Cir. 2007) (holding that there is no First Amendment protection for court testimony given pursuant to official job duties).

[548] *Garcetti*, 547 U.S. at 421-22.

[549] Vladeck, *supra* note 256, at 1540; *see also* Jamie Sasser, *Silenced Citizens: The Post-*Garcetti *Landscape for Public Sector Employees Working in National Security*, 41 U. RICH. L. REV. 759, 760 (2007) (arguing that *Garcetti* bars any First Amendment claim a government employee might make with respect to the unauthorized disclosure of national security information).

[550] Vladeck, *supra* note 256, at 1541.

[551] *See* Kitrosser, *supra* note 13, at 3 (discussing how *Garcetti* has been misinterpreted to apply more broadly than it really does in limiting protection of free speech); Morse, *supra* note 12, at 430 (arguing that *Garcetti* does not undermine the right of national security employees to engage in whistleblowing).

[552] *Garcetti*, 547 U.S. at 422 (explaining that the respondent acted as a federal employee, and not as a citizen, when "conducting his daily professional activities, such as supervising attorneys, investigating charges, and preparing filings").

[553] *Id.* at 424-25.

[554] Lane v. Cent. Ala. Cmty. Coll., 523 F. App'x 709 (11th Cir. 2013), *cert. granted*, No. 13-483, 2013 WL 5675531 (U.S. Jan. 17, 2014) (granting cert on the question of whether a government employee who gave truthful testimony pursuant to a subpoena about information he learned on his job is entitled to any First Amendment protection).

To be sure, *Garcetti* has had a "catastrophic" effect on the free speech rights of public employees.[555] Although the Court couched this new rule in the notion that it would make the government more accountable, it actually has the opposite effect.[556] *Garcetti* has served to strip many government employee-whistleblowers of First Amendment protection for their speech.[557] But this is only because, in those cases, whistleblowing is an expected part of the employees' positions. And I agree that in cases involving high-level government employees who are encouraged to reveal national security information, the employees might have a harder time arguing that these disclosures are not an expected part of their job.[558] If a government employee gives information to the media as part of a coordinated public relations campaign – as some critics claim occurred with leaks during the election about President Obama's role in authorizing drone attacks – there is a decent argument that *Garcetti* would bar any First Amendment claim.[559] But that is because the leaks were arguably made as part of the employee's employment duties. None of the leak prosecutions to date appear to have involved that sort of situation. If anything, the job duties of the prosecuted leakers required them not to disclose information without authorization.

Furthermore, Vladeck's reading of *Garcetti* would strip the First Amendment protections of government employees to a bare nullity. In *Garcetti*, the Court reiterated that government employees frequently have much to contribute to the public debate as a result of their expertise gained through their employment.[560] If government insiders were no longer permitted to share any insights they learn as a result of their employment, the special contribution they could make to the public debate would be minimalized.

B. *Government Insiders and National Security Cases*

The Supreme Court has never directly addressed whether a government insider can find any shelter under the First Amendment for the disclosure of national security information to the press. The most relevant case, *Snepp v. United States*, does not bode well for leakers, but as a civil case, it is distinguishable.[561] Furthermore, the decision is widely out of step with the Court's First Amendment jurisprudence and should be overruled. The only

[555] Paul Secunda, Garcetti*'s Impact on the First Amendment Speech Rights of Federal Employees*, 7 FIRST AMEND. L. REV. 117, 119 (2008).

[556] *Id.*

[557] *Id.*

[558] *Cf.* Bonn v. City of Omaha, 623 F.3d 587, 593 (8th Cir. 2010) (holding that a "Public Safety Auditor" lacked First Amendment protection for releasing a report to the public and discussing it in the media "as a function or official duty of [her] position").

[559] For example, *Garcetti* might also have been an obstacle to any First Amendment claim Scooter Libby might have had regarding his leak about Valerie Plame.

[560] Garcetti v. Ceballos, 547 U.S. 410, 419-20 (2006).

[561] Snepp v. United States, 444 U.S. 507 (1980) (per curiam).

appellate opinion to address the First Amendment rights of government insiders in the context of a criminal prosecution rejected the First Amendment claim before it, but the concurring opinions of two of the three judges on the panel left open the possibility of such a claim in a future case.[562]

1. Civil Cases

One of the strongest arguments the government has to support its position against First Amendment rights for national security employees is *Snepp v. United States*, in which the Supreme Court held that the First Amendment does not invalidate nondisclosure agreements signed by a federal employee that require the employee to obtain prior government approval before publishing any information or materials relating to the employing agency.[563] *Snepp* has been the subject of scathing academic criticism because it is not consistent with the rest of the Court's jurisprudence relating to either government employees or national security information.[564] The decision should be overruled. But even if it is not, it is not clear that it should have any bearing on the First Amendment rights of government insiders who are facing criminal charges based on the disclosure of national security information.

Frank Snepp was a former CIA employee who signed an agreement as a condition of his employment agreeing that he would not publish any information relating to the agency without obtaining the agency's prior approval.[565] The CIA brought a lawsuit to enforce this contract when Snepp published a highly critical book about CIA activities in South Vietnam without first obtaining agency approval.[566] The government wanted a declaration that Snepp had breached his contract, an injunction requiring Snepp to submit his future writings for prepublication clearance, and an order authorizing a constructive trust for the government's benefit over all the past and future profits Snepp earned and would earn from the unauthorized publication of his

[562] United States v. Morison, 844 F.2d 1057, 1081 (4th Cir. 1988) (Wilkinson, J., concurring); *id.* at 1085 (Phillips, J., concurring).

[563] *Snepp*, 444 U.S. at 510.

[564] Emerson, *supra* note 461, at 100 (characterizing *Snepp* as an "aberration"); Goldston et al., *supra* note 14, at 441-42 (arguing that *Snepp* "can hardly be viewed as an authoritative resolution of the first amendment/national security questions in the government employee context" given its unusual procedural posture and cursory attention to the First Amendment questions at issue); *see also* RONALD DWORKIN, A MATTER OF PRINCIPLE 393 (1985) (arguing *Snepp* was "wrong on the merits, and not just as a matter of procedure and remedy"); GREENAWALT, *supra* note 6, at 285 n.2 (stating that the author is "among the many critics who think that the result in that case was far from sufficiently attentive to free speech concerns and that the failure to have full briefing and oral argument was disgraceful").

[565] *Snepp*, 444 U.S. at 507-08. Snepp also signed a similar agreement when he terminated his government position. *Id.* at 508 n.1.

[566] *Id.* at 507.

book.[567] Without the benefit of briefs or oral argument, the Court issued a highly controversial per curiam opinion that turned First Amendment doctrine on its head.[568] As Judge Easterbrook has observed, the Court "treated Snepp's argnments [sic] with disdain."[569] Although the Court had previously set a very high bar for prior restraints in the Pentagon Papers case, the Court rejected Snepp's argument that the agreement amounted to an unconstitutional prior restraint, reasoning that traditional First Amendment principles did not apply because Snepp's employment with the CIA "involved an extremely high degree of trust."[570]

The Court's analysis of the enforceability of a system of prior restraints was relegated to a single footnote that summarily rejected Snepp's constitutional challenge.[571] The Court held that even though the government could not constitutionally prohibit Snepp from publishing unclassified information, the CIA had a right to insist on prepublication review of anything its employees might publish "to ensure *in advance*, and by proper procedures, that information detrimental to national interest is not published."[572] The Court suggested that the government could have required Snepp to submit to prepublication review even in the absence of a signed contract.[573] The Court explained that unclassified material that looks innocuous might, in fact, be harmful in the eyes of experienced CIA officials, because it could lead to the exposure of classified information or sources.[574] It held that the agreement was a "reasonable means" of protecting the government's compelling interest in protecting not only information important to our national security but also the "*appearance* of confidentiality" essential for collecting foreign intelligence.[575] The Court granted the CIA's request for an injunction, requiring Snepp to submit all of his future writings for prepublication review, and imposed a constructive trust on all of Snepp's past and future profits from the sale of his book.[576]

---

[567] *Id.* at 508.

[568] Frank H. Easterbrook, *Insider Trading, Secret Agents, Evidentiary Privileges, and the Production of Information*, 1981 SUP. CT. REV. 309, 339.

[569] *Id.*

[570] *Snepp*, 444 U.S at 510.

[571] Medow, *supra* note 4, at 779.

[572] *Snepp*, 444 U.S. at 513 n.8. The Court noted that prepublication review is a reasonable means of achieving the CIA Director's statutory mandate to "protec[t] intelligence sources and methods from unauthorized disclosure." *Id.* at 509 n.3 (alteration in original) (quoting 50 U.S.C. § 403(d)(3) (1976)).

[573] *Id.* at 509 n.3 ("Moreover, this Court's cases make clear that – even in the absence of an express agreement – the CIA could have acted to protect substantial government interests by imposing reasonable restrictions on employee activities that in other contexts might be protected by the First Amendment.").

[574] *Id.* at 512.

[575] *Id.* at 509 n.3 (emphasis added).

[576] *Id.* at 515-16.

As discussed above, *Snepp* has been the subject of widespread scholarly criticism.[577] The Court did not grapple with a series of difficult questions raised by the enforcement of Snepp's contract.[578] To begin, it is unclear that the CIA had a statutory basis upon which to base its request for injunctive relief. Indeed, attempts to pass legislation that would criminalize the unauthorized dissemination of classified information have failed over and over again; the United States does not have an Official Secrets Act like Britain does. Accordingly, *Snepp* essentially gives the CIA and the executive branch even broader authority to censor its employees than an Official Secrets Act would provide; not only does it punish those who disclose classified information, but it requires all employees to endure a system of prior restraints even when they seek to disclose only unclassified information.[579] When it stated in broad language that the agency had authority to protect the identity of sources, the Court failed to examine whether Congress understood that it was authorizing the CIA to impose an administrative censorship regime.[580] The decision thus stands in marked contrast to the Pentagon Papers case, where a majority of Justices rejected the government's claim for injunctive relief because Congress had not authorized it.[581] Worst of all, the *Snepp* opinion says "nothing about the first amendment; nor does it consider the possibility that Snepp's publication might have value in terms of freedom of expression."[582] The Court also entirely ignored the implications of permitting government employees to contract away their First Amendment rights.[583]

All of the procedural irregularities of the case, as well as its complete disregard of precedent and First Amendment issues, would support the Court's decision to overrule it. At the very least, *Snepp* should be limited to the civil context. Although the Court indicated that the contracts requiring a prior restraint met constitutional scrutiny, it did not address what standard the government must meet to render criminal punishment for the publication of classified information.[584] The distinction between civil sanctions and criminal punishment is extraordinarily important.

3. Criminal Cases

Because the government has either dismissed or obtained guilty pleas in most of its leaker prosecutions to date, there is only one appellate decision addressing whether government insiders have any First Amendment right to

[577] *See supra* note 564 and accompanying text.

[578] Edgar & Schmidt, Jr., *supra* note 186, at 374.

[579] *Id.* at 373-75 ("The Court's opinion gave no sign that a prior restraint mechanism could conceivably pose any problems in terms of traditional first amendment analysis.").

[580] *Id.* at 375.

[581] *Id.*

[582] *Id.*

[583] *Id.* at 373-75.

[584] *See* Snepp v. United States, 444 U.S. 507 (1980) (per curiam).

leak information to the press.[585] As indicated previously, some lower courts have accepted the government's argument that leak prosecutions do not implicate the First Amendment at all.[586] Other courts have recognized that First Amendment rights are at stake but have concluded that the prosecutions before them comported with constitutional requirements.[587]

The leading leaker case is *United States v. Morison*,[588] which concerned a naval intelligence officer who gave satellite photographs of Soviet naval preparations to the British publisher of a periodical about naval operations internationally.[589] In addition to rejecting Morison's statutory arguments that the Espionage Act applied only in traditional espionage cases,[590] the Fourth Circuit also rejected his arguments that the First Amendment provides special protection to disclosures to the press.[591] The court easily distinguished the Pentagon Papers case as a case involving a prior restraint against the press, not a prosecution of a source.[592] In response to arguments that prosecutions of sources could undermine the ability of the press to perform its function, the majority opinion relied on *Branzburg v. Hayes* for the proposition that the First Amendment does not provide the press or its sources with immunity from otherwise valid criminal laws.[593] The court also relied on *Snepp* – although admittedly these cases are not precisely on point – in rejecting Morison's First Amendment defense.[594]

Notably, the two concurring opinions in *Morison* recognized that the charges against Morison implicated the First Amendment. Judge Wilkinson recognized the government's tendency to withhold information from the public and the important role leaks play in fostering democratic accountability.[595] At the same time, he expressed concern for the judiciary's capacity for second-guessing the executive and the ability of "one disgruntled employee" to derail

[585] United States v. Morison, 844 F.2d 1057 (4th Cir. 1988).

[586] *See supra* Part II.A.1.

[587] *See supra* Part II.A.1.

[588] *Morison*, 844 F.2d 1057.

[589] *Id.*

[590] *See supra* Part II.B.3 (discussing the Espionage Act and related statutes).

[591] *Morison*, 844 F.2d at 1068.

[592] *Id.* at 1068; s*ee also id.* at 1081 (Wilkinson, J., concurring) ("No member of the press is being searched, subpoenaed, or excluded, as in a typical right of access case.").

[593] *Id.* at 1068 (majority opinion) ("We do not think that the First Amendment offers asylum under those circumstances, if proven, merely because the transmittal was to a representative of the press." (citing Branzburg v. Hayes, 408 U.S. 665 (1972))).

[594] *Id.* at 1069.

[595] *Id.* at 1081 (Wilkinson, J., concurring) ("There exists the tendency, even in a constitutional democracy, for government to withhold reports of disquieting developments and to manage news in a fashion most favorable to itself. Public debate, however, is diminished without access to unfiltered facts.").

a government program.[596] Furthermore, he was skeptical that the government would ever prosecute someone who revealed wrongdoing given the "political firestorm" that would ensue.[597] In a separate concurrence, Judge Phillips agreed that the First Amendment issues in the case were "real and substantial."[598] Together, the concurring opinions appear to leave open the possibility of a First Amendment defense in a future case.

IV. MAKING DISTINCTIONS

One possible response to the uptick in leak prosecutions is to trust prosecutorial discretion. After all, the government is still not prosecuting the vast majority of leaks. It is unlikely to prosecute leakers who reveal genuine instances of wrongdoing because a jury is unlikely to deliver a guilty verdict in such cases. Indeed, this has been the argument some have made in response to arguments regarding the First Amendment rights of government outsiders.[599]

But, as the Supreme Court has said time and time again, First Amendment rights cannot be left to the whims of prosecutorial discretion.[600] Furthermore, the prosecutions the government has brought hardly give solace that prosecutors will exercise their discretion carefully. During its brief "war on leakers," the government has already demonstrated that it might exercise its discretion to drop a prosecution only after it has already ruined the life of its target. Consider the prosecution of former NSA executive Thomas Drake, who originally faced ten felony charges but ultimately pled guilty to a minor misdemeanor.[601] In response to the government's request for a severe sentence to "send a message" to other government workers, Judge Richard D. Bennett exclaimed that it was "unconscionable" for the government to drag Drake and his family through "four years of hell," only to drop all charges except a misdemeanor count on the eve of trial.[602] As the government recognized at trial, Drake will never work for the federal government again and is now employed as a clerk at an Apple store.[603] The government's decision to charge

[596] *Id.* at 1083.

[597] *Id.* at 1084.

[598] *Id.* at 1085 (Phillips, J., concurring).

[599] *See* SCHOENFELD, *supra* note 6, at 270 (arguing that the government is unlikely to prosecute harmless disclosures or those that reveal wrongdoing).

[600] *See, e.g.*, United States v. Stevens, 130 S. Ct. 1577, 1591 (2010) ("[T]he First Amendment protects against the Government; it does not leave us at the mercy of *noblesse oblige*.").

[601] *Ex-Official at NSA Gets Year of Probation*, WASH. POST, July 16, 2011, at A5.

[602] Transcript of Sentencing Proceeding at 16-17, 28-29, 42, United States v. Drake, No. 1:10-CR-181-RDB (D. Md. July 15, 2011), *archived at* http://perma.cc/FEL2-QFGH.

[603] *Id.* at 35 ("[Defense counsel]: . . . . And as Your Honor pointed out, he had lost his job and government service, a senior executive position, as [the prosecutor] has pointed out, he was a college professor at a university level, and in order to support his family he had to find a job at the Apple Store in retail making an hourly wage.").

Bradley Manning with aiding the enemy also demonstrates prosecutorial zealousness in this area.[604]

As I explain in the prior Section, the argument that government insiders have no First Amendment right to disseminate information without authorization is based on a misunderstanding of First Amendment doctrine. The question remains, however, what sort of First Amendment rights these government insiders do have. As difficult as it is to answer this question, it is essential that we do so, not only to protect individuals from overzealous criminal prosecutions, but also to change the culture within the government so that those who are willing to reveal wrongdoing are encouraged to do so.

Given that the Court has determined that the *Pickering* framework applies to government employee speech claims, and my argument that *Garcetti* would not stand as a bar to a First Amendment claim in most cases, it is tempting to conclude that the same framework should apply in this context. This Section rejects that approach. Using a balancing test to evaluate the First Amendment claims of government insiders would be problematic for a number of reasons. The first is that the test was not developed in the context of a criminal prosecution and is out of step with the rest of the Court's jurisprudence regarding the constitutionality of laws that criminalize speech. The other reason is that a balancing test is unworkable in this context.

Instead, it is essential to distinguish treason and espionage from other types of leaks. Treason and espionage are not "speech" under the First Amendment, but these categories must be carefully defined, just like every category of unprotected speech, so that they apply only in cases where the defendants intended to communicate with a foreign power (or "enemy," in the case of treason). By carefully considering what is disclosed, why it was disclosed, and to whom it was disclosed, it is possible to discern the leaker's intended audience and make the necessary distinctions among leaks. Although the First Amendment permits the government, functioning as an employer, to restrict speech of government insiders more easily than it can restrict the speech of government outsiders, this power should be restricted to the imposition of employment-related civil and administrative sanctions. The Article concludes that government should be entitled to pursue criminal sanctions on government insiders – and outsiders – who are not traitors or spies only when their disclosures pose a direct and irreparable threat to national security that is not outweighed by the public interest in the information.

A. *Civil Versus Criminal Sanctions*

If, as I argue, leakers do not operate entirely outside the protections of the First Amendment, the question remains what rights they do have. It is tempting to argue simply that the *Pickering* balancing test should apply; indeed, some

[604] David S. Cloud, *Wikileaks Probe Brings New Charges; The Army Files 22 More Counts Against a Suspected Leaker, and May Charge Others*, L.A. TIMES, Mar. 3, 2011, at AA6.

scholars have suggested just that.[605] The problem with this argument is that the *Pickering* balancing test arose and has been applied exclusively in the context of challenges to civil sanctions and adverse employment actions, not criminal charges.[606] This makes all the difference in the world. Although, generally speaking, First Amendment rights do not vary based on whether the government seeks to impose a civil or criminal punishment, in the context of government employment, the government should have more power to impose employment-related sanctions on its employees than it should have to impose criminal sanctions.

In the context of national security leaks, scholars have long commented on the potential unfairness of allowing the government to impose criminal penalties for leaks based on the same standard used for civil sanctions,[607] but only recently have scholars begun to focus on whether First Amendment analysis is penalty sensitive.[608] As a general matter, it is certainly true that the Court has never suggested that the First Amendment applies with any less force when the government uses civil rather than criminal sanctions to restrict or compel speech. In other words, it usually does not really matter what kind of punishment an individual receives when determining the scope of his First Amendment rights.[609] Indeed, in *New York Times v. Sullivan*, the Court analogized private causes of action for defamation to criminal charges under the Sedition Act of 1798 and observed that if anything, the lack of the panoply of procedural protections that attach to any criminal charges – but not in civil cases – may render civil claims even more threatening to First Amendment interests.[610] But within the defamation context, the Court has distinguished among compensatory, presumed, and punitive damages and prescribed different levels of fault for the recovery of each.[611] As a result, the state is not

[605] *See, e.g.*, Goldston et al., *supra* note 14, at 438-39 (arguing that applying *Pickering* to national security employees could lead to "a qualified employee right to release information relating to national security").

[606] Kitrosser, *supra* note 13, at 420.

[607] *See, e.g.*, MORTON H. HALPERIN & DANIEL N. HOFFMAN, TOP SECRET: NATIONAL SECURITY AND THE RIGHT TO KNOW 85 (1977); Edgar & Schmidt, Jr., *supra* note 186, at 356; Emerson, *supra* note 461, at 95-96; Nimmer, *supra* note 428, at 331-32 & n.99.

[608] Michael Coenen, *Of Speech and Sanctions: Toward a Penalty-Sensitive Approach to the First Amendment*, 112 COLUM. L. REV. 991, 997 (2012); Kitrosser, *supra* note 13, at 441 ("[C]ourts should consider varying the precise nature of the government's burden with the severity of the penalty sought in the criminal or civil context.").

[609] Coenen, *supra* note 608, at 994.

[610] N.Y. Times Co. v. Sullivan, 376 U.S. 254, 277-78 (1964) (observing that safeguards "such as the requirements of an indictment[,] . . . proof beyond a reasonable doubt," and double-jeopardy do not apply in civil case).

[611] *See, e.g.*, Gertz v. Robert Welch, Inc., 418 U.S. 323, 350 (1974) (requiring actual malice for presumed and punitive damages in private figure/public concern case).

limited in its ability to hold someone liable for defamation, but as the severity of the civil sanction increases, so does the level of fault.[612]

In cases involving the government's various "managerial domains," such as prisons, the military, schools, and government employment, the Court permitted the government to restrict speech in ways that it usually could not, by focusing on the "special circumstances" of these environments.[613] Thus, in the context of student speech rights, the Court has recognized that schools have more leeway to punish student speech with school-related sanctions like suspension or expulsion, but it has never held that students could be criminally or even civilly punished under these lesser standards.[614] Similarly, the Court has permitted searches conducted by school officials on a lower level of scrutiny – reasonableness – than the Fourth Amendment would require if those same searches were performed at the students' homes or by law enforcement officials.[615] None of the Court's government-employee jurisprudence involves the imposition of criminal sanctions based on the *Garcetti-Pickering-Connick* framework.

One can understand why the Court has held that the First Amendment gives the government as employer greater power to restrict the speech of its employees than it is entitled to restrict the speech of ordinary citizens. In its capacity as an employer, the government has a strong interest in having greater hiring and firing control over its employees, just as a private employer would. It does not follow that the government is entitled to control the speech of its employees through criminal sanctions. Indeed, it just cannot be the case that the government can impose criminal sanctions on its employees as long as it meets the relatively low standards of the *Garcetti-Pickering-Connick* framework. After all, this would mean that the government could throw in jail anyone who speaks out of turn in the course of his job duties[616] or speaks on a matter of private concern.[617]

---

[612] *See* Coenen, *supra* note 608, at 1007.

[613] Many scholars have addressed the Supreme Court's tendency to abandon its usual First Amendment principles and analysis in the context of speech restrictions in various government institutions. *See, e.g.*, C. Thomas Dienes, *When the First Amendment Is Not Preferred: The Military and Other "Special Contexts*,*"* 56 U. CIN. L. REV. 779 (1988); Gia Lee, *First Amendment Enforcement in Government Institutions and Programs*, 56 UCLA L. REV. 1691 (2009); Scott A. Moss, *Students and Workers and Prisoners—Oh, My! A Cautionary Note About Excessive Institutional Tailoring of First Amendment Doctrine*, 54 UCLA L. REV. 1635 (2007); Lawrence Rosenthal, *The Emerging First Amendment Law of Managerial Prerogative*, 77 FORDHAM L. REV. 33 (2008); Frederick Schauer, *Toward an Institutional View of the First Amendment*, 89 MINN. L. REV. 1256 (2005).

[614] *See* Mary-Rose Papandrea, *Student Speech Rights in the Digital Age*, 60 FLA. L. REV. 1027, 1038-56 (2008).

[615] New Jersey v. T.L.O., 469 U.S. 325, 341 (1985).

[616] *See* Garcetti v. Ceballos, 547 U.S. 410, 426 (2006).

[617] *See* Connick v. Myers, 461 U.S. 138, 154 (1983).

Furthermore, as a public policy matter, one might wonder whether the government even needs criminal sanctions to control the dissemination of information effectively. After all, the threat of dismissal and the loss of a security clearance should be sufficient deterrents to most government insiders who consider revealing national security information without authorization.[618] Criminal sanctions would seem to be unnecessary overkill. If criminal laws have even greater deterrent value, they might over-deter leaks, and overdeterrence is a significant problem when the public relies so heavily on leaks to inform public debate. In addition, the truly massive number of leaks and the limited prosecutorial resources that could realistically be devoted to prosecuting leaks necessarily lead to concerns about selective prosecution.[619]

Permitting criminal sanctions for leaks only in extraordinary circumstances would also reduce the threat to the media. As we have seen with the recent spate of leak prosecutions, the government is likely to subpoena reporters and news organizations to obtain the identity of a leaker. In addition, these reporters and media outlets potentially face criminal charges of their own for inchoate crimes like conspiracy and aiding and abetting.[620]

B. *The Problem with Balancing Tests*

Another reason not to use the *Pickering* balancing test in the context of criminal prosecutions is that it would offer relatively uncertain and weak protection for constitutional rights. Furthermore, requiring courts to weigh the value of the leak's contribution to the public discourse against the harmfulness of the leak is unworkable.

One hallmark of a balancing test is the lack of certainty that it provides; a potential leaker would have a difficult time predicting at the outset whether his leak would be protected.[621] That much is true for any balancing test, and especially for any public employee seeking protection under *Pickering*.

---

[618] *See* Emerson, *supra* note 461, at 97.

[619] *See id.* at 96 ("[T]he amount of information which slips through the government's fingers is so enormous, the system of leaks so pervasive, and the possibility of stemming the tide so out of reach, that application of criminal sanctions for divulging information would hardly be workable. Prosecutions would be highly selective, thereby unfair, and subject to serious abuse.").

[620] *See id.*

[621] *See* Harry Kalven, Jr., *The* New York Times *Case: A Note on "The Central Meaning of the First Amendment,"* 1964 SUP. CT. REV. 191, 212 (observing that self-censorship results when individuals refrain "from uttering what was in fact true 'because of doubt whether it can be proved in court or fear of the expense of having to do so'" (quoting N.Y. Times Co. v. Sullivan, 376 U.S. 254, 279 (1964))); Lee, *supra* note 4, at 1489; Melville B. Nimmer, *The Right to Speak from Times to Time: The First Amendment Applied to Libel and Misapplied to Privacy*, 56 CALIF. L. REV. 935, 939 (1968). Categorical rules that provide no protection whatsoever for leaked information would of course provide the benefit of certainty. Lee, *supra* note 4, at 1489.

Although the public school teacher in *Pickering* prevailed, the Court has been increasingly deferential to employee assertions in subsequent cases.

In the national security context, courts are likely to be even more deferential given their general reluctance to second guess the executive branch on national security issues.[622] Furthermore, any ad hoc balancing test will be hostage to the public values and anxiety of the time.[623] For example, in times of terrorist activity, the public – the jury – is less likely to be sympathetic to a government insider who reveals an arguably illegal government program that is aimed at reducing terrorism. In *Dennis v. United States*,[624] for example, the Court applied an ad hoc balancing test and ended up affirming the defendants' convictions for forming the Communist party because it was believed that the party posed a threat to the security of the nation.[625]

An additional problem with applying *Pickering* is that the test is not well designed to balance the value of the information against the harmfulness of the information. Instead, courts tend to focus on whether the disclosure undermines the effective functioning of the government. In light of *Snepp*, courts are likely to credit the government's assertion that leaks of any sort – even if they do not concern classified information and even if they are not particularly newsworthy – undermine the proper functioning of the government. In the Court's view, proper functioning depends upon not only the need for the secrecy of sensitive national security information but also "the *appearance* of confidentiality so essential to the effective operation of our foreign intelligence service."[626] Furthermore, even if a court is willing to balance the value of the disclosed information against the harmfulness of disclosure, it is not clear how a court would conduct that balance.

In the context of civil sanctions, applying *Pickering* would be preferable to the current approach,[627] but for all the reasons above, a balancing test remains deeply problematic. That said, when applied properly, the test should be useful for leakers in some limited instances. For example, government insiders should be permitted to argue that the information at issue was improperly classified

[622] Lee, *supra* note 4, at 1489 ("[B]alancing is unlikely to accomplish much because courts are likely to defer to the expertise of intelligence agencies on matters such as the harmfulness of a leak."); *see, e.g.*, Dep't of Navy v. Egan, 484 U.S. 518, 530 (1988) ("[U]nless Congress specifically has provided otherwise, courts traditionally have been reluctant to intrude upon the authority of the Executive in military and national security affairs."); SAGAR, *supra* note 85, at 55-65.

[623] Methven, *supra* note 466, at 91.

[624] 341 U.S. 494 (1951).

[625] *Id.* at 516-17 ("[Petitioners'] conspiracy to organize the Communist Party and to teach and advocate the overthrow of the Government of the United States by force and violence created a 'clear and present danger' of an attempt to overthrow the Government by force and violence.").

[626] Snepp v. United States, 444 U.S. 507, 510 n.3 (1980) (per curiam) (emphasis added); *see also* CIA v. Sims, 471 U.S. 159, 175 (1985) (citing this language from *Snepp* favorably).

[627] *See* Kitrosser, *supra* note 13.

and/or already in the public domain. Furthermore, the government should not be entitled to punish disclosers who have an objectively reasonable belief that they have revealed the violation of a law, rule, or regulation, an instance of gross mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety. The person who leaks to the press should be protected as long as that person can demonstrate that it would have been futile to follow internal reporting procedures. When these conditions are met, the value of the speech, and the speaker's interest in speaking, outweigh the government's interest in silencing the speaker.

C. *Standard for Criminal Sanctions*

If the Bradley Manning prosecution is any indication, the government is likely to pursue constitutional or military treason charges against a leaker again, particularly if the leaker chooses to disclose information to the public through a foreign, new media entity like WikiLeaks. Despite the government's arguments to the contrary, a meaningful distinction exists between treason and espionage on the one hand, and leaking to the public on the other. It is time for both our statutes and First Amendment doctrine to reflect this distinction.

Ideally, Congress should rewrite the Espionage Act and related statutes to make a clear distinction between disclosures that are intended to reach the enemy and those that are intended to inform the American public. Given that statutory reform is not likely to occur in the near future, it is essential for courts to rethink the First Amendment implications of leak prosecutions. Although treason and espionage are not constitutionally protected, these categories need to be carefully defined. Other leaks should not be criminally actionable unless they pose a direct and grave danger to the nation's security that is not outweighed by the public's interest in the information.

1. Distinguishing Treason and Espionage

The government is plainly correct that information published in the *New York Times* is just as likely to fall into our enemies' hands as if a spy hand delivered the secrets directly to them. But as a matter of public policy and First Amendment doctrine, there is an essential distinction between treason and espionage, and information disclosed to the public at large.

Although treason is distinct from espionage, the two crimes overlap because they both involve communication directed to a foreign power. Treason is a more limited crime because it requires that the information be aimed at an "enemy," while espionage can occur even when our secrets are disclosed to our allies. The other significant difference between treason and espionage is that treason requires adherence to the enemy.

Information disclosed directly and solely to a foreign power does not enrich the public debate in any way; information disclosed to the public often does. Private disclosures are unlikely to serve the public interest, but are more likely to serve the interests of the leaker and the entity receiving the disclosure. Public disclosures, on the other hand, may potentially benefit every foreign

adversary. As discussed in Part I.B.4, the publication of information to the general public is crucially different from disclosures to the press. When disclosures are made to the press, the government knows what the enemies know. In the case of traditional espionage, the government does not know what secrets have been compromised.[628]

Of course, this distinction is more easily made in theory than in fact because traitors and spies certainly can use even traditional media to pass information to the enemy and other nations. In the digital age, the best and most practical way to distinguish between traitors and spies and those attempting to communicate with the public is to focus on the intent of the leaker and the identity of the recipient of the disclosures.

To avoid a conflict with the First Amendment, the crime of treason must be limited to those instances when the defendant has a specific intent to aid the enemy. In cases where the defendant is serving as an agent or employee of a foreign nation, the inquiry will be easy. In other cases, it will be essential to look at extrinsic evidence to determine whether this specific intent exists. Not only is it impossible to get inside someone's mind, but it is also too easy for defendants to assert at trial that their primary goal was to inform the American public. Most leak cases so far have not gone to trial, but in those that have – *Morison* and *Manning* – the courts did consider extrinsic evidence regarding the purpose for the disclosures. Although determining intent can be tricky, these cases demonstrate that it can be done. Furthermore, in other contexts – especially employment discrimination – courts have proven to be well equipped to determine the primary motivation for defendants' actions.

Evidence that the leaker had "bad" motivations – like a desire to get revenge on superiors, or achieve some level of notoriety – should be taken into account just as bad motivations are taken into account in defamation cases. In defamation cases, desire to harm an individual is not by itself evidence of bad intent, but it can be considered in sorting out the true intent of the actor.[629] Similarly, in leak cases, a "bad" motive standing alone should not strip government insiders of their constitutional protections, but instead should be relevant in determining the leaker's intent.

In addition to defendants' own explanations for their actions, courts should consider what was disclosed and to whom. By looking at what is disclosed, the factfinder can make some conclusions regarding the intent of the leaker. Disclosures of potentially illegal government activities, like those involved in the Snowden leaks, will generally support arguments that the leaks were made to inform the American public and not aid the enemy. Indiscriminate information dumps, like Manning's, raise a red flag regarding the leaker's intent, although such acts by themselves will not be determinative.[630] In

[628] *See supra* note 230 and accompanying text.

[629] Harte-Hanks Commc'ns, Inc. v. Connaughton, 491 U.S. 657, 667-68 (1989).

[630] In comparison, Snowden does not appear to have disseminated documents indiscriminately. He contends he had "all sorts of documents" he did not turn over; instead,

considering the context of the disclosures, a court should factor in the public value of the information. Information that is not particularly illuminating for public debate is less likely to be intended for public consumption.

A leaker's choice of forum – "to whom" the disclosures were made – should be considered as one of the most helpful factors in determining whether the leaker was acting with the intent of communicating with the public. The problem in the digital age is that it is difficult, if not next to impossible, to determine which publications should be regarded as members of the press operating with the intention to communicate with the general public, or at least a relevant subset of the public. Indeed, this is very similar to the inquiry that is plaguing courts and legislatures grappling with whether to recognize a reporters' privilege.[631] This may require courts to inquire whether the entity engages in "journalism" and to conduct a careful inquiry into the audience the leaker intended to reach through his communications. Bradley Manning made a persuasive argument that disclosing information to WikiLeaks was not much different from disclosing the information to a more traditional news outlet because, in many ways, at the time of his disclosures, WikiLeaks served as an important watchdog function throughout the world and, in fact, had won awards for its reporting.[632]

In some cases it will not be as difficult to determine whether the leaker hopes to stir public debate. The Snowden leaks are a perfect example. Although commentators and public officials continue to call him a traitor because he escaped to Hong Kong and then Russia,[633] his decision to enlist the help of Glenn Greenwald at the *Guardian* and Barton Gellman at the *Washington Post* is strong evidence of intent to inform the public about controversial government surveillance activities.[634] The benefits of revealing information through major newspapers are obvious. In addition to reaching the broadest possible audience and avoiding online obscurity, disclosing information through traditional media takes advantage of journalists' expert ability to provide a broader context and meaning to complex documents.[635]

---

he contends, he "evaluated every single document I disclosed to ensure that each was legitimately in the public interest." Glenn Greenwald et al., *supra* note 222.

[631] I discuss this problem at length elsewhere. *See* Mary-Rose Papandrea, *Citizen Journalism and Reporters' Privilege*, 91 MINN. L. REV. 515 (2006).

[632] For a lengthier discussion of the problems distinguishing WikiLeaks from the traditional media, see Mary-Rose Papandrea, *The Publication of National Security Information in the Digital Age*, 5 J. NAT'L SECURITY L. & POL'Y 119 (2011); Benkler, *supra* note 24.

[633] Will Englund, *Snowden Stayed at Russian Consulate*, WASH. POST, Aug. 27, 2013, at A3. If evidence emerges that Snowden shared information with foreign countries directly, his claims about his intent to inform the American public will certainly be suspect. At this time, however, the government does not appear to have any evidence that this is the case.

[634] Greenwald et al., *supra* note 222 (quoting Snowden as saying "[m]y sole motive is to inform the public").

[635] *See* Rusbridger, *supra* note 109, at 31.

Disclosing the information to more than one news organization, as both Daniel Ellsberg and Snowden did, does little to undermine this objective evidence of the leaker's intent. Multiple disclosures guards against the chances that any one news outlet will be unable or unwilling to publish due to government pressure, threats of criminal prosecution, or court injunction.[636]

In addition, evidence that a government insider tried to disclose information to the traditional media is relevant to the intent inquiry, although, by itself, it should not defeat, or prove, treason or espionage charges.[637] In the *Manning* case, the defense argued that Manning had first tried to pass along the information to the *New York Times*, the *Washington Post*, and *Politico*, but he gave the information to WikiLeaks only after he felt a *Washington Post* reporter did not take him seriously, no one at the *New York Times* returned his calls, and bad weather hampered his efforts to deliver documents to *Politico*.[638]

Indeed, courts should not assume that a government insider who reveals information directly (for example, through a personal blog) lacks the requisite intent to communicate with the American public. Indeed, some whistleblowers have felt that they had no other choice than to make their disclosures themselves. For example, in 2004, Lockheed Martin employee Michael DeKort uploaded a video to YouTube outlining various safety and security deficiencies of ships his employer was making for the Coast Guard.[639] In the video, DeKort stated, "I have exhausted every avenue I can think of."[640] DeKort had bought his concerns to the CEO and Board of Directors of Lockheed Martin, as well as the Inspector General for the Department of Homeland Security and congressmen.[641] DeKort said that the company rebuffed his concerns because the project was over budget and behind schedule.[642] In addition, DeKort claimed that the Inspector General (IG) had investigated his concerns for six months but then told DeKort that the IG could not do anything to address them due to "lack of cooperation from the U.S. Coast Guard,"[643] though the IG denied that.[644] When asked why he had not

[636] *Id.*

[637] After all, a government insider could try to plant information in the traditional media as a means of reaching a foreign government.

[638] Ed Pilkington, *Manning Says He First Tried to Leak to* Washington Post *and* New York Times, GUARDIAN (Feb. 28, 2013), http://www.theguardian.com/world/2013/feb/28/manning-washington-post-new-york-times, *archived at* http://perma.cc/HGN2-FB96.

[639] Michael DeKort, YOUTUBE (Aug. 3, 2006), http://www.youtube.com/watch?v=qd3VV8Za04g.

[640] *Id.*

[641] Griff Witte, *On YouTube, Charges of Security Flaws*, WASH. POST, Aug. 29, 2006, at D1.

[642] *Id.*

[643] *See* DeKort, *supra* note 639.

[644] *See* Witte, *supra* note 641.

taken his concerns to the press, DeKort said that the institutional media was not interested in publishing his allegations because they did not believe him.[645]

Down the road, there will be cases where government insiders disclose national security information through a media entity that is publically accessible yet affiliated with – or at least sympathetic to – our nation's enemies. In such cases, it will be essential to examine closely both the nature of the publication to which the leaks were made as well as the government insider's reasons for sharing information with that particular information distributor in order to determine whether the disclosures were made to aid our enemies, or to inform the American public.

2. All Other Leaks

Leaks that do not fall within the categories of treason or espionage constitute "speech" under the First Amendment. Furthermore, the Court's jurisprudence giving the government as employer greater leeway to sanction the speech of its employees is in the context of employment-related sanctions. When it comes to criminal sanctions, the government should not be permitted to punish its employees criminally unless the government makes the same showing it must make for government outsiders.

This conclusion begs the question: What standard the government must meet in the context of government outsiders? Unfortunately, there is no clear answer. I argue elsewhere that the same high standard for prior restraints – grave and direct harm to national security – should apply in any criminal prosecution of government outsiders.[646] Although this was the standard the Supreme Court set for prior restraints in the Pentagon Papers case, and even though the Court specifically left open the possibility of subsequent criminal charges based on a lesser showing, the distinction between prior restraints and subsequent criminal punishment is not significant enough to justify a distinction between the two.[647] As the Pentagon Papers case demonstrated, requiring direct and grave harm to national security is essential in order to prevent the government from overreaching. True, it can be difficult at times to determine whether a disclosure actually poses a direct risk of a serious harm to national security, but when there is uncertainty, the benefit of the doubt should tip in favor of protecting First Amendment rights. In most cases, the government will not be able to meet this burden.

In cases where the government can demonstrate a direct and grave harm to national security interests, it should also be required to demonstrate that the

[645] *60 Minutes: The Troubled Waters of "Deepwater"* (CBS television broadcast May 17, 2007), *archived at* http://perma.cc/DP44-BPN2 (stating that the press said DeKort's allegations – including his claim that Lockheed Martin had ordered radios that were not waterproof – seemed "a little too fantastic").

[646] *See* Papandrea, *supra* note 3, at 298.

[647] *Id.* at 280-81.

public interest in the information did not outweigh the harm.[648] The question of the public's interest does not come into play unless and until the government has demonstrated harm. The Court did not discuss the role of a public interest inquiry in the Pentagon Papers case, but that is no doubt because the government had not demonstrated the requisite level of harm. Balancing the value of the information against its harm is a tricky and complicated task. It will occur, however, only in cases in which the government has shown grave harm, and, in such instances, will protect defendants only when the disclosures reveal some sort of government wrongdoing.

Applying the same high standard in criminal prosecutions involving government insiders and outsiders will make it more difficult for the government. With respect to government insiders, however, the government will maintain the ability to impose civil sanctions based on a much lower standard. These sanctions – such as the loss of employment – are by no means trivial and will have a significant deterrent effect on potential leaks.

CONCLUSION

This Article contends that the First Amendment rights of government insiders are substantial. Although treason and espionage are not "speech" under the First Amendment, these categories must be carefully defined to apply only in cases where the defendant intended to communicate with a foreign entity. By carefully considering what was disclosed, why it was disclosed, and to whom it was disclosed, it is possible to discern the leaker's intent and distinguish among treason, espionage, whistleblowing, and other leaks.

By recognizing that even national security employees have some First Amendment protection to reveal classified information in support of their reports of wrongdoing, courts would not merely save some individual employees from adverse employment actions and prosecution, but would also potentially change the internal cultural norms of the national security workplace.[649] With that change, we can come closer to achieving the appropriate balance between secrecy and transparency.

---

[648] *See* Geoffrey R. Stone, *Government Secrecy vs. Freedom of the Press*, 1 HARV. L. & POL'Y REV. 185, 204 (2007) ("[T]o justify the criminal punishment of the press for publishing classified information, the government must prove that the publisher knew that (a) it was publishing classified information, (b) . . . which would result in likely, imminent, and serious harm to the national security, *and* (c) . . . would not meaningfully contribute to public debate.").

[649] Lobel, *supra* note 202, at 48; *see also* Daniel Ellsberg, *Secrecy and National Security Whistleblowing*, 77 SOC. RES. 773 (2010).