ESPIONAGE 2.0: PROTECTING HUMAN INTELLIGENCE SOURCES IN THE DIGITAL AGE

KIMBERLEY A. CHURCH*

TABLE OF CONTENTS

* Class of 2012, University of Southern California Gould School of Law; B.A. History of Art and Architecture, B.A. Psychology, University of California Santa Barbara. I am grateful to Professor Rebecca Lonergan for her invaluable guidance in writing this Note, to my family for their unwavering support, and to the staff and editors of the *Southern California Law Review*.

I. INTRODUCTION

> National security of the United States has been put at risk . . . . The lives of people who work for the American people have been put at risk. The American people themselves have been put at risk by these actions that I believe are arrogant, misguided and ultimately not helpful in any way. We are doing everything that we can.
>
> —Eric Holder, United States Attorney General, on the release of 250,000 State Department cables by WikiLeaks.[1]

On November 28, 2010, the international whistleblower website WikiLeaks and five major newspapers began simultaneously publishing confidential diplomatic cables from 270 U.S. embassies around the world.[2]

1. *Holder: 'Significant' Actions Taken in WikiLeaks Investigation*, CNN.COM (Dec. 6, 2010), http://politicalticker.blogs.cnn.com/2010/12/06/skip-to-main-content-cnn-cnn-us-edition-u-s-international-mexico-set-edition-preference-sign-up-log-in-home-video-newspulse-u-s-wor/.

2. Scott Shane & Andrew W. Lehren, *Leaked Cables Offer Raw Look at U.S. Diplomacy*, N.Y. TIMES (Nov. 28, 2010), http://www.nytimes.com/2010/11/29/world/29cables.html. The five newspapers are the *New York Times*, *The Guardian*, *Der Spiegel*, *El País*, and *Le Monde*. Eric Schmitt, *Air Force Blocks Sites That Posted Secret Cables*, N.Y. TIMES (Dec. 14, 2010), http://www.nytimes.com/2010/12/

The cables were originally obtained by WikiLeaks, which also posted the cables on its own website.[3] Over 100,000 of the cables in WikiLeaks' possession are classified, with 15,000 classified as "secret,"[4] meaning their release could reasonably be expected to cause serious damage to the national security.

The cables can allegedly be traced back to a single source: Bradley Manning, a former U.S. Army intelligence analyst. Since the leak, the Pentagon has announced new measures to protect against similar breaches. Even with secure technology, however, so long as there are government secrets there will always be the risk of leaks—whether inadvertently, purposefully with good intentions, or purposefully with intent to harm the United States. Moreover, in the digital age, governments face a new threat: opportunities to publish leaked classified information have multiplied, as evidenced by so-called "internet drop-boxes," which can post thousands of secret documents in only a matter of seconds for all the world to see. Never before has there been such a powerful tool for undermining government secrecy.

Historically, courts have refused to enjoin publishers from revealing classified information, and in today's digital era, an injunction would likely be ineffective against new media outlets, which are often operating abroad in secret. Criminal law is the government's best remedy for punishing leaks of this nature. Under current U.S. law, however, the federal government is largely unable to punish the unauthorized publication of classified information absent intent or reason to believe that it will be used to harm the United States. In other words, if a publisher asserts a proper purpose for releasing classified information, such as informing the public, that publisher cannot be punished even if responsible for the release of hundreds of thousands of classified documents. The only exception to this rule is if the classified information concerns "communications intelligence" activities—in that case, the government need not prove an improper purpose because such information is extremely vital to the United States and vulnerable to unauthorized leaks.

This Note argues that Congress must enact such a criminal law specifically designed to protect classified information concerning human intelligence sources and methods. Part II begins with an overview of the

15/us/15wiki.html.

3. *Secret US Embassy Cables*, WIKILEAKS, http://wikileaks.org/cablegate/html (last visited Apr. 17, 2012).

4. *Id.*

media, distinguishing traditional media outlets, such as the *New York Times*, from new websites, such as WikiLeaks, that indiscriminately, anonymously, and continuously publish secret information. In Part III, this Note describes how the U.S. government protects its secrets, both in the executive branch by establishing a system for classifying sensitive information, and in the legislative branch by promulgating a series of statutes that criminally punish acts of espionage. Since courts have yet to interpret the espionage statutes as applied to the media, Part III outlines how courts have applied and construed these statutes in other contexts. Part IV explores how courts balance First Amendment rights of free speech with the government's interest in national security, and Part V explains why, on balance, prior restraints against new media outlets like WikiLeaks are legally tenable but nevertheless problematic given that a new media outlet would probably not respect a court order enjoining it from publishing sensitive information.

This Note concludes in Part VI and VII that in light of the changing face of the media, Congress should permit criminal sanctions against the media for publishing classified information related to human intelligence sources and methods. Such an amendment to current espionage laws will strike the proper balance between the First Amendment and the government's interest in national security while effectively deterring new media outlets such as WikiLeaks from publishing a particularly vulnerable category of classified information.[5]

II. NEW MEDIA

The face of the media has changed. In the past, the public relied primarily on newspapers to stay informed of the government's affairs. Today, technology is inextricably integrated into our daily lives.[6] Nearly half of the American public downloads most of its news about national and

5. For an account of WikiLeaks and historical precedent, see generally Sandra Davidson, *Leaks, Leakers, and Journalists: Adding Historical Context to the Age of WikiLeaks*, 34 HASTINGS COMM. & ENT. L.J. 27 (2011). For an argument in support of refined classification and declassification procedures in light of WikiLeaks, see generally Wendy J. Keefer, *Protection of Information to Preserve National Security: Is WikiLeaks Really the Issue?*, 5 CHARLESTON L. REV. 457 (2011), and for an argument that the government should focus on properly defining what constitutes a "media organization," see generally Jamie L. Hester, *The Espionage Act and Today's "High-Tech Terrorist,"* 12 N.C. J.L. & TECH. ONLINE 177 (2011).

6. *See* Doug Meier, Note, *Changing with the Times: How the Government Must Adapt to Prevent the Publication of Its Secrets*, 28 REV. LITIG. 203, 212 (2008) (noting that the paradigmatic shift from old media to new media has changed the way people interact with one another).

international issues on the Internet[7] where people can access a seemingly endless amount of information in an instant. The Internet also provides an unprecedented international forum for sharing ideas and information. Everybody has a voice: a visitor to a website can respond in real time to articles, blog posts, and videos.[8] Common phrases like "citizen journalism"[9] capture the collaborative nature of the new Internet-based media. New media has also radically changed our concept of journalism, which used to be a term reserved for skilled, professionally trained reporting typically performed for news outlets such as newspapers and magazines. But in this new interactive paradigm where everyone can be a journalist, nothing is guaranteed to be accurate. Articles are not necessarily written by educated, unbiased journalists, and information is not necessarily published to benefit and inform society.[10]

With the new media frontier also come new opportunities for espionage and, more specifically, the anonymous publication of classified information. Websites such as WikiLeaks serve as a clearinghouse for the world's secrets. WikiLeaks is an international website that posts secret material submitted by anonymous sources. The website's claimed purpose is to "let whistleblowers . . . post sensitive documents on the Internet without being traced."[11] By promising anonymity to its sources, WikiLeaks has gained significant popularity among leakers: within only one year of its launch in 2006, the WikiLeaks database contained over one million secret documents.[12] Although WikiLeaks does not actively solicit information,[13] it is designed precisely to elicit leaks by providing a "high security

7. Jolie O'Dell, *For the First Time, More People Get News Online than from Newspapers*, MASHABLE.COM (Mar. 14, 2011), http://mashable.com/2011/03/15/online-versus-newspaper-news/.

8. *See* C.W. Anderson, *Data, Diffusion, Impact: Five Big Questions the Wikileaks Story Raises About the Future of Journalism*, NEIMAN JOURNALISM LAB (Jul. 26, 2010, 1:00 PM), http://www.niemanlab.org/2010/07/data-diffusion-impact-five-big-questions-the-wikileaks-story-raises-about-the-future-of-journalism/ (discussing this phenomenon in the context of the WikiLeaks-Afghanistan story).

9. *Citizen Journalism*, WIKIPEDIA, http://en.wikipedia.org/wiki/Citizen_journalism (last visited June 2, 2012). Wikipedia is the largest and most successful example of citizen journalism, with its open publishing and collaborative editing. *See id.*

10. Meier, *supra* note 6, at 212.

11. *Chinese Cyber-Dissidents Launch WikiLeaks, a Site for Whistleblowers*, THE AGE (Jan. 11, 2007, 7:35 AM), http://www.theage.com.au/news/Technology/Chinese-cyberdissidents-launch-WikiLeaks-a-site-forwhistleblowers/2007/01/11/1168105082315.html [hereinafter *Chinese Cyber-Dissidents Launch Wikileaks*].

12. Steven Aftergood, *Wikileaks and Untraceable Document Disclosure*, SECRECY NEWS (Jan. 3, 2007), http://www.fas.org/blog/secrecy/2007/01/wikileaks_and_untraceable_docu.html.

13. *See What Is Wikileaks?*, WIKILEAKS, http://www.wikiLeaks.org/About.html (last visited June 2, 2012) ("Like other media outlets conducting investigative journalism, we accept (but do not solicit) anonymous sources of information.").

anonymous drop box fortified by cutting-edge cryptographic information technologies," giving "maximum protection to [its] sources."[14] Indeed, WikiLeaks' sole purpose is the collection and publication of secrets.

The Internet enables WikiLeaks to operate entirely behind closed doors; most of its members work secretly in different parts of the world. Likewise, WikiLeaks' database is compartmentalized so that if one server goes down (or if the entire site is shut down) its secret-keeping mechanism will remain safe. The clandestine operation even claims to have an "insurance" file: if anything happens to its founder, Julian Assange, or the website, WikiLeaks will release the key that decrypts a cache of uncensored documents already posted on its site.[15] Assange specifically warned that efforts to curtail his activities could trigger a "deluge of national and commercial secrets."[16]

Finally, unlike more traditional media outlets, WikiLeaks publishes troves of uncensored material instantaneously. On the one hand, this provides the public with an unfiltered lens into the inner workings of the governments and corporations that shape our daily lives. The public's "right to access" information about its government enables meaningful control over the process of governance.[17] On the other hand, the potential cost of indiscriminate, unfettered, and unredacted publication is staggering because it can reveal ongoing military operations and intelligence activities.

A. A CLOSER LOOK AT WIKILEAKS

Although WikiLeaks initially focused on oppressive regimes in Asia, the former Soviet Union, sub-Saharan Africa, and the Middle East,[18] the website is best known for its leaks related to the United States, particularly military activities in Iraq and Afghanistan and diplomatic reports compiled by the State Department. These leaks brought WikiLeaks international attention, beginning with its release in April 2010 of a video showing a

14. *Id.*

15. *WikiLeaks 'Insurance' File Aimed at Ensuring Work Goes On*, MSNBC.COM (Dec. 5, 2010, 3:14:07 AM), http://www.msnbc.msn.com/id/40512398/ns/us_news-wikileaks_in_security/t/wikileaks-insurance-file-aimed-ensuring-work-goes/#.T8qzubDbA1M [hereinafter MSNBC.COM]. Tens of thousands of people have already downloaded the "insurance" file, making it impossible to contain in the event WikiLeaks releases the decryption key. *Id.*

16. *Id*.

17. *See* Press-Enter. Co. v. Super. Ct. of Cal., 464 U.S. 501, 517, 519 (1984) (Stevens, J., concurring).

18. *Chinese Cyber-Dissidents Launch WikiLeaks*, *supra* note 11.

helicopter attack that killed nearly twenty civilians in Baghdad, Iraq, including two Reuters news correspondents.[19] In July of the same year, WikiLeaks released a compilation of over 91,000 documents related to the Afghanistan war going back to 2004.[20] In October, the site released nearly 400,000 documents related to the war in Iraq.[21] Then, on November 28, WikiLeaks began releasing 250,000 U.S. State Department cables.[22] These leaks brought WikiLeaks and its leader, Julian Assange, both significant praise and vitriol.

Each of these four leaks can allegedly be traced back to Private First Class Bradley Manning, a former intelligence analyst in the U.S. Army. Manning is said to have first contacted WikiLeaks in November 2009 from his workstation in Iraq,[23] where he had access to the Secret Internet Protocol Router Network ("SIPRNet")—a system of interconnected computer networks used by the U.S. military since the mid-1990s to transmit classified information at the confidential and secret levels.[24] After the 9/11 terrorist attacks, the U.S. intelligence community was criticized for its failure to share data that may have prevented the attacks;[25] in response,

19. *Timeline: WikiLeaks Founder in Jail*, REUTERS (Dec. 9, 2010, 8:46 AM), http://www.reuters.com/article/2010/12/09/us-wikileaks-assange-events-idUSTRE6B741R20101209.

20. *Id.*

21. *Id. See also* Bill Brenner, *The WikiLeaks Drama: A Timeline*, CSO ONLINE (Dec. 9, 2010), http://www.csoonline.com/article/645707/the-wikileaks-drama-a-timeline?page=1 (providing another timeline of significant WikiLeaks events).

22. Brenner, *supra* note 21.

23. DAVID LEIGH & LUKE HARDING, WIKILEAKS: INSIDE JULIAN ASSANGE'S WAR ON SECRECY 31 (2011). Manning's arrest and alleged involvement was first announced by Wired.com. Kevin Poulsen & Kim Zetter, *U.S. Intelligence Analyst Arrested in Wikileaks Video Probe*, WIRED.COM (June 6, 2010, 9:31 PM), http://www.wired.com/threatlevel/2010/06/leak/. For an account of the bizarre way in which Manning's alleged involvement came to light, see Glenn Greenwald, *The Strange and Consequential Case of Bradley Manning, Adrian Lamo and Wikileaks*, SALON.COM (June 18, 2010, 5:20 AM), http://www.salon.com/2010/06/18/wikileaks_3/; Jonathan V. Last, *The Left's Canonization of St. Bradley Manning*, CBS NEWS (Jan. 11, 2011, 8:30 AM), http://www.cbsnews.com/stories/2011/01/11/opinion/main7233405.shtml.

24. Clark Boyd, *Tech Podcast: SIPRnet and the WikiLeaks Cables*, PRI'S THE WORLD (Dec. 3, 2010), http://www.theworld.org/2010/12/tech-podcast-siprnet-and-the-wikileaks-cables/; U.S. DEP'T OF THE ARMY, 2005 DEFENSE BASE CLOSURE AND REALIGNMENT COMMISSION REPORT 22 (2007), *available at* http://www.defense.gov/brac/pdf/Report-Closure-FortMonmouth.pdf. For a discussion of the U.S. government classification system, see *infra* Part III.A.

25. *See* NAT'L COMM'N ON TERRORIST ATTACKS UPON THE U.S., THE 9/11 COMMISSION REPORT 403 (2004), *available at* http://govinfo.library.unt.edu/911/report/911Report.pdf (noting that the problem of coordinating agencies is "nearly intractable because of the way the government is currently structured" and that "[i]t is hard to break down stovepipes when there are so many stoves that are legally and politically entitled to have cast-iron pipes of their own") (internal quotation marks omitted); Anthony Kimery, *Information Technology: An End to Infosharing?*, HOMELAND SECURITY TODAY (Feb. 1, 2011), http://www.hstoday.us/focused-topics/information-technology/single-article-page/an-end-to-infosharing/55915db66128bc355cd71ca0eeb13a6a.html ("The failure to connect the

access to SIPRNet was expanded to U.S. embassies and State Department personnel.[26] By expanding access to the system, however, SIPRNet became more vulnerable to unauthorized leaks.[27]

Each of the four leaks tied to Manning is described in detail below.

1. Collateral Murder

In April 2010, WikiLeaks posted to its website classified footage from a July 12, 2007 Baghdad airstrike in which nineteen civilians were killed by an Apache helicopter, including two war correspondents for Reuters.[28] The video, titled by WikiLeaks as "Collateral Murder," was shot from the helicopter's cockpit gun-sight and depicted a series of three airstrikes. In the first strike, the helicopter opened fire on a group of ten men, two of whom were armed: one with a rocket-propelled grenade launcher and another with an AK-47 assault rifle. Two Reuters journalists were caught in the fire—one was carrying a camera that may have been mistaken for a weapon.[29] In total, nine people were killed in this first strike. The second and third strikes resulted in ten additional deaths.[30] WikiLeaks was heavily criticized for selectively editing the video footage to focus on the journalists caught in the gunfire, rather than the armed men.[31] Assange admitted, however, that he was seeking to manipulate public opinion and create "maximum political impact."[32]

2. Afghanistan War Diary

On July 25, 2010, WikiLeaks published 75,000 of some 91,000 U.S. military war logs covering the war in Afghanistan from 2004 to 2010.[33]

dots of the 9/11 plot was due in large part to analysts' inability to easily and quickly access the intelligence they needed. This intelligence was contained in a hodge-podge of disparate, unlinked and incompatible computer systems and databases.").

26. Boyd, *supra* note 24. *See also* Julian Borger & David Leigh, *Siprnet: Where America Stores Its Secret Cables*, THE GUARDIAN (U.K.) (Nov. 28, 2010, 1:15 PM), http://www.guardian.co.uk/world/2010/nov/28/siprnet-america-stores-secret-cables (discussing SIPRNet in greater detail).

27. *See* Kimery, *supra* note 25.

28. *Collateral Murder*, WIKILEAKS, http://collateralmurder.com (last visited June 2, 2012).

29. *Id.*

30. *Id.*

31. Toby Harnden, *Julian Assange's Arrest Warrant: A Diversion from the Truth?*, THE TELEGRAPH (U.K.) (Aug. 22, 2010, 10:54 PM), http://www.telegraph.co.uk/technology/news/7959227/Julian-Assanges-arrest-warrant-a-diversion-from-the-truth.html.

32. *Id.*

33. *Afghan War Diary, 2004–2010*, WIKILEAKS (July 25, 2010), http://mirror.wikileaks.info/wiki/Afghan_War_Diary,_2004-2010. WikiLeaks has delayed releasing the remaining 15,000 documents as part of a "harm minimization process demanded by [their] source," stating that the

The so-called "Afghan War Diary" reveals information on the unreported deaths of civilians, increased Taliban attacks, and involvement by Pakistan and Iran in the insurgency. The *New York Times* described the Diary as an "archive of classified military documents [which] . . . offers an unvarnished, ground-level picture of the war in Afghanistan that is in many respects more grim than the official portrayal."[34]

Most of the documents in the Afghan War Diary are classified "secret"—the second of three tiers in the U.S. classification system.[35] The U.S. government urged WikiLeaks to return the approximately 92,000 documents and condemned the website for publishing them, arguing that by doing so WikiLeaks placed the lives of Americans and its partners at risk and threatened the United States' national security.[36] As the National Security Advisor in the White House pointed out, however, the Afghan War Diary covered a time period when the war in Afghanistan was under-resourced, and President Barack Obama had since initiated a new strategy allocating new resources to the war "precisely because of the grave situation [in Afghanistan]."[37] Another U.S. official downplayed the leak's impact on U.S. foreign policy and national security interests, stating, "I don't think anyone who follows this issue will find it surprising that there are concerns about [Pakistan's Inter-Services Intelligence] and safe havens in Pakistan. In fact, we've said as much repeatedly and on the record."[38] As one senior Afghan official pointed out, however, this leak will "further limit the [United States'] access to the uncensored views of Afghans."[39] Defense Secretary Robert Gates lamented that the trust between the Afghan people and the U.S. military has been breached: "[I]n the intelligence business . . . the sacrosanct principle is protecting your sources . . . . [A]s a result of this massive breach of security, [the United States has] considerable repair work to do in terms of reassuring people and rebuilding

documents will eventually be released as the security situation in Afghanistan permits. *Id.*

34. C.J. Chivers et al., *The Afghan Struggle: A Secret Archive and an Unvarnished View*, N.Y. TIMES, Jul. 26, 2010, at A1.

35. *See infra* Part III.A for a detailed overview of the U.S. classification system.

36. Chivers et al., *supra* note 34, at A8.

37. THE WHITE HOUSE, U.S. CENTRAL COMMAND, STATEMENT OF NATIONAL SECURITY ADVISOR GENERAL JAMES JONES ON WIKILEAKS, http://www.centcom.mil/news/statement-of-national-security-advisor-gen-james-jones-on-wikileaks (last visited June 2, 2012).

38. Mike Allen, *White House Condemns 'Irresponsible' Leaks, Dismisses Stories*, POLITICO (Jul. 25, 2010, 7:15 PM), http://www.politico.com/news/stories/0710/40204.html.

39. Tom Coghlan & Giles Whittell, *Afghan Informants' Lives at Risk from Documents Posted on WikiLeaks*, THE AUSTRALIAN (Jul. 28, 2010, 11:24 AM), http://www.theaustralian.com.au/news/world/afghan-informants-lives-at-risk-from-documents-posted-on-wikileaks/story-e6frg6so-1225897924552.

trust."[40]

Others confirmed that the Afghan War Diary's publication poses a serious risk of harm to informants and other civilians whose identities were revealed in the documents. One newspaper claims it took just two hours of sifting through the Diary to identify dozens of Afghans credited with providing detailed intelligence to U.S. forces.[41] In many cases, their villages and fathers' names were given for identification as well. Even when names were redacted, in some cases enemy militants could still discover the identity of a "traitor."[42] Indeed, immediately after WikiLeaks published the Diary, the Taliban confirmed that it was analyzing the documents and intended to hunt down and punish any suspected spies.[43] Julian Assange defended WikiLeaks, arguing that the need to inform the public outweighs this risk: "[O]ur understanding of the material is that it's vastly more likely to save lives than cost lives."[44] Assange also proclaimed that many informers in Afghanistan acted "in a criminal way" by sharing false data with NATO authorities and blamed the White House for not helping WikiLeaks check the data prior to its release.[45]

3. Iraq War Logs

On October 22, 2010, WikiLeaks released classified U.S. Army field reports of the war in Iraq from 2004 to 2009 (the "Iraq War Logs").[46] The reports describe incidents as documented by U.S. military personnel on the ground in Iraq. Most notably, the reports detail the abuse and torture of prisoners by Iraqi forces and the reckless behavior of private security contractors.

This time, WikiLeaks more vigorously redacted identifying information of civilians implicated in the reports. Its motivation for doing

40. Ravi Somaiya, *Taliban Says It Will Target Names Exposed by WikiLeaks*, NEWSWEEK (Jul. 30, 2010, 6:31 AM), http://www.newsweek.com/2010/07/30/taliban-says-it-will-target-names-exposed-by-wikileaks.html.

41. Coghlan & Whittell, *supra* note 39. The *New York Times*, *The Guardian*, and *Der Spiegel* also published excerpts of the Afghan War Diary but did not publish the names of individual Afghans. Eric Schmitt & David E. Sanger, *Gates Cites Peril in Leak of Afghan War Logs*, N.Y. TIMES, Aug. 2, 2010, at A4, *available at* http://www.nytimes.com/2010/08/02/world/02wiki.html.

42. Coghlan & Whittell, *supra* note 39.

43. Somaiya, *supra* note 40.

44. Kris Jepson, *Wikileaks: Damage Is Done Say Human Rights Group*, CHANNEL 4 NEWS, http://www.channel4.com/news/articles/politics/international_politics/wikileaks+damage+already+done+says+human+rights+group/3727677.html (last updated Jul. 29, 2010).

45. *Id.*

46. *Baghdad War Diary*, WIKILEAKS, http://wikileaks.org/irq/ (last visited June 2, 2012).

so, however, was not to reduce the risk of loss of life but rather to prevent any "distractions" from the content of the material.[47] The reports temporarily complicated negotiations to form a new government in Iraq but otherwise largely repeated what had already been reported in the mainstream media.[48]

4. Cablegate

On November 28, 2010, WikiLeaks began publishing classified U.S. State Department cables originating from 274 embassies, consulates, and diplomatic missions.[49] The published cables, collectively called "Cablegate," cover a period of over forty years, beginning in December 1966 and ending in February 2010,[50] with well over half from 2007 or later.[51] While many of the 251,287 cables in WikiLeaks' possession are unclassified, 101,748 are classified confidential, and 15,652 are classified secret.[52] Nine thousand cables are labeled "noforn," meaning the contents are considered "too delicate to be shared with any foreign government," and 4000 are designated both "secret" and "noforn."[53]

Many of the cables reveal the names of U.S. diplomats' confidential sources, including foreign legislators, military officers, human rights activists and journalists, often with an explicit warning to protect the sources' confidentiality.[54] A small sampling of the leaked cables reveals the breadth of information they cover, from nuclear fuel in Pakistan, to financial support of Al Qaeda by Saudi donors, to speculation about a "close relationship" between the Italian prime minister, Silvio Berlusconi, and the Russian prime minister, Vladimir Putin.[55] Some cables reveal

47. Larry Shaughnessy, *WikiLeaks Redacted More Information in Latest Documents Release*, CNN.COM (Oct. 23, 2010), http://edition.cnn.com/2010/US/10/22/wikileaks.editing/. Julian Assange stated that

> [i]n this case we have taken an even more vigorous approach than we took in relation of the Afghan material, not because we believe that approach was particularly lacking [but] rather just to prevent those sort of distractions from the serious content by people who would like to try and distract from the message.

Id.

48. Editorial, *Wikileak's Leaks Mostly Confirm Earlier Iraq Reporting*, WASH. POST (Oct. 26, 2010), http://www.washingtonpost.com/wp-dyn/content/article/2010/10/25/AR2010102504643.html. *See also* Michael R. Gordon & Andrew W. Lehren, *Reports Trace the Role of Iran as a Backer of Shiite Militias*, N.Y. TIMES, Oct. 23, 2010, at A1 (summarizing and analyzing the content of the reports).

49. *Secret US Embassy Cables*, *supra* note 3.

50. *Id*.

51. Shane & Lehren, *supra* note 2.

52. *Secret US Embassy Cables*, *supra* note 3.

53. Shane & Lehren, *supra* note 2.

54. *Id.*

55. *Id.*

insights and tactics in U.S. foreign relations. One such series of cables recounts U.S. officials' meetings in September 2009 and February 2010 with Ahmed Wali Karzai, a "power broker" in Kandahar and the half-brother of the president of Afghanistan.[56] In the cables, the U.S. diplomats cautioned that Karzai is widely known to be a narcotics trafficker and revealed that they believed some of his statements to be false.[57] They also speculated that Karzai was unaware that the United States had this information and reported that they would continue to monitor his activity.[58]

The White House denounced WikiLeaks' release of the cables as a "reckless and dangerous action," warning that some cables could disrupt intelligence operations and place the lives of confidential sources at risk.[59] As one member of the intelligence community explained,

> the leaking of these cables . . . has done great harm to [the United States'] diplomacy, because it strikes at the heart of what diplomacy is: The building of trust between people and between governments. The leaks violate that trust and are going to make some people . . . much more reluctant to discuss their affairs with American diplomats.[60]

Many leaders in the intelligence community have called for action, but the current remedies available to the U.S. government are limited.

III. NATIONAL SECURITY INFORMATION AND THE PROTECTION OF SECRETS IN THE UNITED STATES

A. CATEGORIES OF NATIONAL SECURITY INFORMATION

Three terms are commonly used to refer to national security information in different contexts: national defense information, state secrets, and classified information. While there is some overlap (for example, a classified document may reveal information related to the national defense), distinctions must be drawn between each of these terms to better understand how the U.S. government currently protects against the unauthorized publication of national security information and to ultimately expose gaps in the current statutory framework.

56. *Id.*

57. *Id.*

58. *Id.*

59. Press Release, Office of the Press Sec'y, The White House (Nov. 28, 2010), *available at* http://www.whitehouse.gov/the-press-office/2010/11/28/statement-press-secretary.

60. Michael A. Lindenberger, *The U.S.'s Weak Legal Case Against WikiLeaks*, TIME (Dec. 9, 2010), http://www.time.com/time/nation/article/0,8599,2035994,00.html#ixzz17gXNzX2o.

National defense information ("NDI") broadly describes information related to the military and national preparedness.[61] Although courts typically defer to the executive branch in determining what constitutes NDI,[62] the broad scope NDI encompasses also implies some additional demonstration of potential harm to the nation on the part of the government.[63] NDI may leave unprotected certain kinds of information that do not relate to the national defense but are nevertheless important to the national security.[64] For example, NDI may exclude nonmilitary government secrets vital to the country's foreign affairs and intelligence activities.[65]

The state secrets privilege is a common law privilege designed to prevent courts from revealing secrets in the course of civil litigation that would harm national security. This evidentiary privilege was first recognized in *United States v. Reynolds*, which held that the government may prevent the disclosure of certain evidence if there is a reasonable danger that the disclosure "will expose military matters which, in the interest of national security, should not be divulged."[66] In *Reynolds*, plaintiffs in a tort action sought production of accident reports concerning the crash of a B-29 airplane that killed three civilians on board.[67] The Air Force refused to comply with the trial court's order to produce the reports, arguing that releasing details of the crash would harm national security.[68] The trial court granted a directed verdict against the government and the Third Circuit Court of Appeals affirmed,[69] but the Supreme Court reversed.[70] In outlining the state secrets privilege, the Court stated that "[t]he privilege belongs to the Government and must be asserted by it," but cautioned that it "is not to be lightly invoked"[71] and that "[i]n each case,

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

62. *See, e.g.*, United States v. Morison, 844 F.2d 1057, 1082 (4th Cir. 1988) (Wilkinson, J., concurring) ("In the national security field, the judiciary has performed its traditional balancing role with deference to the decisions of the political branches of the government.").

63. *See id.* at 1071–72 (upholding jury instructions requiring the government to prove that the information's disclosure would be potentially damaging to the United States or useful to an enemy of the United States).

64. Eric E. Ballou & Kyle E. McSlarrow, Note, *Plugging the Leak: The Case for a Legislative Resolution of the Conflict Between the Demands of Secrecy and the Need for an Open Government*, 71 VA. L. REV. 801, 808–09 (1985).

65. *Id.*

66. United States v. Reynolds, 345 U.S. 1, 10 (1953).

67. *Id.* at 1–3.

68. *Id.* at 1, 5.

69. *Id.* at 5.

70. *Id.* at 12.

71. *Id.* at 7.

the showing of necessity . . . will determine how far the court should probe in satisfying itself that the occasion for invoking the privilege is appropriate."[72]

Classified information is a specific subset of national security information, the public disclosure of which could be particularly harmful to the United States and therefore warrants stronger protection against release. Unlike NDI, the government must take affirmative steps to classify information. The current classification system was established by President Franklin D. Roosevelt shortly before the United States entered World War II.[73] Since then, it has been modified by several presidents, most recently by President Barack Obama with Executive Order 13,526.[74]

Under the current classification system, information can only be classified if its unauthorized disclosure would "reasonably be expected to cause identifiable or describable damage to the national security."[75] If there is "significant doubt about the need to classify the information, it shall not be classified."[76] Similarly, information can only be classified if it fits into a specifically enumerated category such as military plans, intelligence activities, sources or methods, and foreign relations or foreign activities of the United States.[77]

Information can be classified at one of three levels: confidential, secret, or top secret. At each classification level, the person classifying the information must be able to identify and describe the risk of damage to national security, and if there is significant doubt about the appropriate level of classification, the information must be classified at a lower level.[78] "Confidential" is the lowest classification level. It applies to information "which reasonably could be expected to cause damage to the national security.[79] "Secret" classification applies to information "which reasonably

72. *Id.* at 11. In *Reynolds*, the necessity was "greatly minimized" by an available alternative—the Air Force offered to make the surviving crew members available for examination. *Id.* Also, there was nothing in the record indicating that the electronic equipment "had any causal connection with the accident." *Id.*

73. Exec. Order No. 8381, 5 Fed. Reg. 1147 (Mar. 26, 1940), *superseded by* Exec. Order No. 10,104, 15 Fed. Reg. 597 (Feb. 1, 1950). President Roosevelt's new classification system was designed to protect "certain vital military and naval installations and equipment." *Id.*

74. Exec. Order No. 13,526, 75 Fed. Reg. 707 (Dec. 29, 2009) (codified as amended at 32 C.F.R. § 2001 (2010)).

75. *Id.* at 709.

76. *Id.* at 707.

77. *Id.* at 709.

78. *Id.* at 708.

79. *Id.* at 708.

could be expected to cause *serious* damage to the national security."[80] "Top secret" classification is reserved for information "which reasonably could be expected to cause *exceptionally grave damage* to the national security." [81] Only certain individuals have the authority to classify information. For example, only the president, vice president, or agency heads or officials may delegate authority to classify information "top secret."[82] Classification authorities must receive yearly training on proper classification and declassification procedures.[83]

Equally important to the proper classification of sensitive information is the declassification of such information as soon as public dissemination no longer poses a threat to the national security. Many of the recent changes to the classification system established more liberal declassification policies. [84] Under the current classification order, an authority classifying information must identify when the information will be declassified.[85] If the classification authority cannot determine a specific date or event for declassification, then the information may be marked for declassification up to twenty-five years from the date of classification.[86] Information can only remain classified for more than twenty-five years if it "should clearly and demonstrably be expected to reveal the identity of a confidential human source or a human intelligence source or key design concepts of weapons of mass destruction."[87] Information may never remain classified indefinitely. [88] The classification system also provides a mechanism for challenging the classification status of information.[89]

Authorized access to classified information is limited to an individual who has (1) been granted a security clearance by the applicable agency; (2) signed a nondisclosure agreement; (3) received training on the proper safeguarding of classified information and on the sanctions that may be imposed for failure to protect classified information from unauthorized disclosure; and (4) has a "need-to-know" the information.[90] Need-to-know

80. *Id.* at 707–08 (emphasis added).
81. *Id.* at 707 (emphasis added).
82. *Id.* at 708.
83. *See id.*
84. For example, President Obama mandated the establishment of a National Declassification Center at the National Archives to "streamline declassification processes, facilitate quality-assurance measures, and implement standardized training regarding the declassification of records." *Id.* at 719.
85. *Id.* at 709.
86. *Id.*
87. *Id.*
88. *Id.*
89. *Id.* at 711.
90. *Id.* at 720.

depends on the functions of the pertinent agency and the roles and responsibilities of the individual requiring access to the classified information.[91] Restrictions on the handling of classified information also protect against its unauthorized release, including how and where it may be stored, how it may be transported, and with whom it may be shared.[92]

Despite these comprehensive policies, leaks inevitably still occur. Thus, Congress has enacted a series of statutes to criminally sanction the unauthorized disclosure and, in some cases, the publication of national security information.

B. STATUTORY PROTECTION AGAINST ESPIONAGE

The Espionage Act[93] was passed in 1917 after heated debate, which stretched over two congressional sessions and encompassed three bills.[94] The Act made certain information-gathering activities criminal when performed with "intent or reason to believe that the information . . . is to be used to the injury of the United States, or to the advantage of any foreign nation" and proscribed the unlawful communication or mishandling of NDI.[95] Congress has since expanded the Act, most notably in the 1950s in response to the Cold War.[96] The espionage statutes are currently codified in 18 U.S.C. §§ 792–799.[97]

1. Section 793: Gathering, Transmitting or Losing Defense Information

Section 793 of the Espionage Act protects against the gathering, transmittal, and loss of NDI. Subsections 793(a), (b), and (c) prohibit, respectively, obtaining information by physical intrusion,[98] copying or

91. 32 C.F.R. § 2001.40(d) (2010).

92. *See id.* §§ 2001.40–2001.55.

93. 18 U.S.C. §§ 792–799 (2006).

94. Harold Edgar & Benno C. Schmidt, Jr., *The Espionage Statutes and Publication of Defense Information*, 73 COLUM. L. REV. 929, 940 (1973).

95. Espionage Act, ch. 30, 40 Stat. 217 (1917) (codified as amended in scattered sections of 22 U.S.C. & 50 U.S.C.).

96. Internal Security Act of 1950, ch. 1024, 64 Stat. 987 (codified at 50 U.S.C. §§ 831–835 (2006)).

97. Other espionage statutes not relevant for purposes of this Note concern harboring or concealing persons, photographing and sketching defense installations, the publication and sale of those images, and violating regulations of the National Aeronautics and Space Administration. *See* 18 U.S.C. §§ 792, 795–797, 799 (2006). For a thorough discussion of the espionage statutes, including legislative histories and judicial interpretations, see generally Edgar & Schmidt, *supra* note 94.

98. Subsection 793(a) reads,

> Whoever, for the purpose of obtaining information respecting the national defense with intent or reason to believe that the information is to be used to the injury of the United States, or to

otherwise obtaining NDI such as writings, sketches, maps, and photographs,[99] and receiving any document or other tangible item if the recipient knows or has reason to believe that the document has been or will be taken or disposed of in violation of the espionage statutes.[100] Each act is criminal only if it was done "for the purpose of obtaining information respecting the national defense *with intent or reason to believe* that the information is to be used to the injury of the United States, or to the advantage of any foreign nation."[101]

Subsections 793(d) and (e) prohibit the willful communication of NDI to any person not entitled to receive it.[102] Communicating NDI is criminal if the individual communicating it has reason to believe that the information could be used to the injury of the United States or to the advantage of any foreign nation.[103] This culpability standard is lower than the standard articulated in § 793(a), (b), and (c): to be criminal, an individual who unlawfully *communicates* NDI need only have reason to believe the information could be used to the injury of the United States or to the advantage of any foreign nation.[104]

> the advantage of any foreign nation, goes upon, enters, flies over, or otherwise obtains information concerning any vessel, aircraft, work of defense, . . . building, . . . or other place connected with the national defense owned or constructed, or in progress of construction by the United States or under the control of the United States . . . [s]hall be fined under this title or imprisoned not more than ten years, or both.

18 U.S.C. § 793(a) (2006).

99. Subsection 793(b) reads,

> Whoever, for the [same purpose stated in § 793(a)], and with like intent or reason to believe, copies, takes, makes, or obtains, or attempts to copy, take, make, or obtain, any sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, document, writing, or note of anything connected with the national defense . . . [s]hall be fined under this title or imprisoned not more than ten years, or both.

Id. § 793(b).

100. Subsection 793(c) reads,

> Whoever, for the [same purpose stated in § 793(a)] receives or obtains . . . from any source whatever, any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note, of anything connected with the national defense, knowing or having reason to believe, at the time he receives or obtains, or agrees or attempts to receive or obtain it, that it has been or will be obtained, taken, made, or disposed of by any person contrary to the provisions of this chapter . . . [s]hall be fined under this title or imprisoned not more than ten years, or both.

Id. § 793(c).

101. *Id.* §§ 793(a)–(c) (emphasis added).

102. Subsection 793(d) relates to communication of NDI by persons with lawful possession, whereas 793(e) relates to communication of NDI by persons with unlawful possession.

103. *See id.* § 793(d)–(e).

104. *Id.* Subsection 793(e) reads,

> Whoever having unauthorized possession of, access to, or control over any document, . . . or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not

2. Section 794: Gathering or Delivering Defense Information to Aid a Foreign Government

Section 794 pertains to what most would consider classic espionage: the communication of NDI to a foreign government with intent or reason to believe that it will be used against the United States. Subsection 794(a) relates to the communication of NDI to any foreign nation at any time,[105] whereas § 794(b) relates to the communication of NDI to an enemy during a time of war.[106] Violation of § 794 is punishable by death or imprisonment for any term of years or for life, except that the death penalty is only available for a violation of § 794(a) upon finding that the offense resulted in the death of a covert agent or directly concerns nuclear weapons or other particularly sensitive types of information.[107]

3. Section 798: Unlawful Disclosure of Classified Information

Section 798 relates to the unlawful disclosure of certain types of classified information. As noted in Part II.A, classified information is a specific subset of national security information, the public disclosure of

entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it . . . [s]hall be fined under this title or imprisoned not more than ten years, or both.

Id. § 793(e).

105. Subsection 794(a) reads,

Whoever, 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, communicates, delivers, or transmits . . . to any foreign government, . . . or to any representative, officer, agent, employee, subject, or citizen thereof, either directly or indirectly, any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, note, instrument, appliance, or information relating to the national defense, shall be punished by death or by imprisonment for any term of years or for life . . . .

Id. § 794(a).

106. Subsection 794(b) reads,

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

Id. § 794(b).

107. *Id.* § 794(a) ("[T]he sentence of death shall not be imposed unless . . . the offense resulted in the identification by a foreign power . . . of an individual acting as an agent of the United States and consequently in the death of that individual, or directly concerned nuclear weaponry, military spacecraft or satellites, early warning systems, or other means of defense or retaliation against large-scale attack; war plans; communications intelligence or cryptographic information; or any other major weapons system or major element of defense strategy.").

which would be particularly harmful to the United States and therefore warrants stronger protection against release. Section 798 prohibits the knowing and willful disclosure or publication of certain types of classified information when the disclosure is prejudicial to the safety or interests of the United States or benefits any foreign nation to the detriment of the United States.[108] Violation of this section is punishable by imprisonment of ten years or less, a fine, or both. Section 798 has a lower culpability standard as compared to § 793 and § 794—the disclosure of classified information need not be done with intent to harm the United States or even with reason to believe that it will be used to the injury of the United States. To violate § 798, rather, the disclosure need only be willful and knowing. Finally, § 798 explicitly proscribes publication, thereby avoiding ambiguity regarding whether or not Congress intended that the statute apply to the press.[109]

In light of the lower culpability standard in § 798, it is important to note the limited scope of this section. First, § 798 only relates to classified information, rather than to NDI in general. This places the onus on the government to take steps in protecting sensitive information in order to bring it within the ambit of the statute. Second, § 798 only proscribes the disclosure of specific categories of classified information, namely, information concerning cryptographic systems and information concerning communications intelligence activities[110] of the United States or any foreign government. Communications intelligence ("COMINT") includes information derived from intercepted communications transmissions.[111] COMINT targets "voice and teleprinter traffic, video, Morse code traffic, or even facsimile messages" collected from the "air waves, cable, fiber optics, or any other transmission medium."[112] As the House Judiciary Committee pointed out when enacting § 798, COMINT is "both vital and

108. Section 798(a) reads,

> Whoever knowingly and willfully communicates, furnishes, transmits, or otherwise makes available to an unauthorized person, or publishes, or uses in any manner prejudicial to the safety or interest of the United States or for the benefit of any foreign government to the detriment of the United States any [specific categories of] classified information . . . [s]hall be fined under this title or imprisoned not more than ten years, or both.

Id. § 798(a).

109. *See id.*

110. As defined in the statute, "communication intelligence" means "all procedures and methods used in the interception of communications and the obtaining of information from such communications by other than the intended recipients." *Id.* § 798(b).

111. INTERAGENCY OPSEC SUPPORT STAFF, SECTION 2: INTELLIGENCE COLLECTION ACTIVITIES AND DISCIPLINES, *in* OPERATIONS SECURITY: INTELLIGENCE THREAT HANDBOOK (1996), *available at* http://www.fas.org/irp/nsa/ioss/threat96/part02.htm [hereinafter INTELLIGENCE THREAT HANDBOOK].

112. *Id.*

vulnerable to an almost unique degree."[113]

a. Human Intelligence

Another intelligence system that is both extremely vital to the national security and vulnerable to leaks is human intelligence ("HUMINT"), "the oldest method for collecting information about a foreign power."[114] HUMINT refers to intelligence gathering by means of interpersonal contact, typically through interrogations and conversations with persons who have access to pertinent information.[115] The manner in which HUMINT operations are conducted is dictated by both official protocol and the nature of the source of the information.[116] Sources may be neutral, friendly, or hostile and may not be aware of their involvement in the collection of intelligence information.[117] Sources must be protected from disclosure that could compromise other intelligence operations or create security threats to the sponsoring nation.[118] Moreover,

> [e]ven with the explosion of technical capabilities, HUMINT can still provide information that even the most proficient technical collectors cannot, such as access to internal memoranda and to compartmented information. Most importantly, human collectors can provide key insights into the intentions of an adversary, whereas technical collection systems are often limited to determining capabilities.[119]

b. Proposed Amendment to § 798: The SHIELD Act

In December 2010, U.S. Senator John Ensign introduced a bill to address unauthorized disclosures of classified information related to human intelligence activities. The Securing Human Intelligence and Enforcing Lawful Dissemination Act ("SHIELD Act") would amend § 798 of the espionage statutes, making it a crime to knowingly and willfully publish classified information "concerning the human intelligence activities of the United States or any foreign government," or "concerning the identity of a classified source or informant of an element of the intelligence community of the United States."[120] Human intelligence is defined in the proposed bill

113. H.R. Rep. No. 81-1895, at 2 (1950).
114. INTELLIGENCE THREAT HANDBOOK, *supra* note 111.
115. *Id.*
116. *Id.*
117. *Id.*
118. *Id.*
119. *Id.*
120. Securing Human Intelligence and Enforcing Lawful Dissemination Act, S. 4004, 111th Cong. § 2(a)(4) (2010). The bill was also introduced in the House of Representatives. H.R. 6506, 111th Cong. § 2 (2010). The SHIELD Act was reintroduced in both houses of Congress in February, 2011.

as "all procedures and methods employed in the collection of intelligence through human sources."[121] "Informant" is defined as "any individual who furnishes information to an intelligence agency in the course of a confidential relationship protecting the identity of such individual from public disclosure."[122]

The proposed bill would also add "transnational threat" to the list of uses of classified information that trigger the statute's applicability. As defined in the proposed bill, "transnational threat" means "any transnational activity (including international terrorism, narcotics trafficking, the proliferation of weapons of mass destruction and the delivery systems for such weapons, and organized crime) that threatens the national security of the United States; or any individual or group that engages in a [transnational activity]."[123]

This change is probably intended to ensure that disclosure of information covered by the statute will be punishable regardless of whether the benefited group purports to govern any territory.[124] With this addition, the statute would read,

> Whoever knowingly and willfully communicates, furnishes, transmits, or otherwise makes available to an unauthorized person, or publishes, or uses in any manner prejudicial to the safety or interest of the United States or for the benefit of any foreign government *or transnational threat* to the detriment of the United States any [specific categories of] classified information . . . [s]hall be fined under this title or imprisoned not more than ten years, or both.[125]

In a House hearing on the proposed legislation, constitutional scholar Geoffrey R. Stone testified that the SHIELD Act is "plainly unconstitutional" as applied to nongovernment individuals who publish or disseminate classified information.[126] As this Note will show, however, it is

See S. 315, 112th Cong. (2011); H.R. 703, 112th Cong. (2011).

121. S. 4004 § 2(b).

122. The SHIELD Act applies the National Security Act's definition of "informant." *See* 50 U.S.C. § 426(6) (2006).

123. S. 4004.

124. Otherwise, such punishment might be considered a restriction of speech based on the content of the speech or the identity of the speaker. *See* JENNIFER K. ELSEA, CONG. RESEARCH SERV., R 414049, CRIMINAL PROHIBITIONS ON THE PUBLICATION OF CLASSIFIED DEFENSE INFORMATION 9 (2010), *available at* http://assets.opencrs.com/rpts/R41404_20101018.pdf.

125. *See* 18 U.S.C. § 798 (2006); S. 4004(a).

126. *Espionage Act and the Legal and Constitutional Issues Raised by Wikileaks: Hearing Before the H. Comm. on the Judiciary*, 111th Cong. 11 (2010) (statement of Geoffrey R. Stone, Professor of Law, University of Chicago), *available at* http://judiciary.house.gov/hearings/printers/111th/111-160_63081.PDF.

unclear how courts would interpret this statute in light of the First Amendment when a member of the media is implicated.[127] Further, even if the SHIELD Act is unconstitutional as applied to more traditional media, it could be applied to a new media outlet such as WikiLeaks when it demonstrates both the means and purpose of undermining the United States' national security, irrespective of whether its activities serve the public's interest.

C. PROSECUTIONS UNDER THE ESPIONAGE STATUTES

Prosecutions under the espionage statutes are rare. Violations are difficult to prove, and the government will face "difficult problems of balancing the need for prosecution and the possible damage that a public trial will require by way of the disclosure of vital national interest secrets in a public trial."[128] Nevertheless, the espionage statutes have successfully weathered several constitutional challenges on First Amendment grounds, such as vagueness and overbreadth.[129]

1. Case Law Interpreting § 793

United States v. Morison is the only case in which a person was convicted of espionage for turning over classified documents to the media. In *Morison*, the Fourth Circuit Court of Appeals upheld the conviction of a Naval Intelligence Support Center employee for stealing classified photographs and selling them to a British publication.[130] The court rejected the defendant's argument that § 793 only applies to "classic spying and espionage activity": "The language of the . . . statute[ ] includes no limitation to spies or to an agent of a foreign government, . . . and [it] declare[s] no exemption in favor of one who leaks to the press. It covers

127. *See infra* Part IV.

128. *See* United States v. Morison, 844 F.2d 1057, 1067 (4th Cir. 1988) (citing Haig v. Agee, 453 U.S. 280 (1981)).

129. United States v. Rosen, 445 F. Supp. 2d 602, 613 (E.D. Va. 2006). *See* Gorin v. United States, 312 U.S. 19 (1941) (rejecting a vagueness challenge to the phrase "information relating to the national defense"); Schenck v. United States, 249 U.S. 47 (1919) (upholding the Espionage Act's constitutionality against a First Amendment challenge); *Morison*, 844 F.2d 1057 (rejecting vagueness and First Amendment challenges to § 793 by a naval intelligence officer who transmitted classified satellite photographs of Soviet naval preparations to a British periodical); United States v. Truong, 629 F.2d 908, 919 (4th Cir. 1980) (rejecting overbreadth challenge to scienter requirement of "reason to believe").

130. *Morison*, 844 F.2d at 1060–61. For a thorough discussion of the background of *Morison*, see GABRIEL SCHOENFELD, NECESSARY SECRETS: NATIONAL SECURITY, THE MEDIA, AND THE RULE OF LAW 223–31 (2010).

anyone."[131]

The *Morison* court also rejected the defendant's assertion that the First Amendment shielded him from liability. Quoting the Supreme Court's landmark 1972 decision in *Branzburg v. Hayes*, the court reiterated that

> [a]lthough stealing documents . . . could provide newsworthy information, neither reporter nor source is immune from conviction for such conduct, whatever the impact on the flow of news . . . . The [First] Amendment does not reach so far as to override the interest of the public in ensuring that neither reporter nor source is invading the rights of other citizens through reprehensible conduct forbidden to all other persons . . . . [H]owever complete is the right of the press to state public things and discuss them, that right, as every other right enjoyed in human society, is subject to the restraints which separate right from wrong-doing.[132]

Section 793's constitutionality was reaffirmed in the more recent and controversial "*AIPAC Case*." In August 2005, the government indicted two lobbyists from the American Israel Public Affairs Committee ("AIPAC").[133] The AIPAC lobbyists, Steven J. Rosen and Keith Weissman, were charged with conspiracy to disclose national defense information to unauthorized individuals including Israeli officials, other AIPAC personnel, and the *Washington Post*.[134] Rosen and Weissman argued that § 793 cannot constitutionally apply to persons, like themselves, who have no "special relationship to the government."[135] In a lengthy opinion, the district court carefully examined prior courts' interpretations of § 793 as well as the statute's legislative history before holding that "both common sense and the relevant precedent point persuasively to the conclusion that the government can punish those outside of the government for the unauthorized receipt and deliberate retransmission of information relating to the national defense."[136]

Although the district court held that § 793 could constitutionally be applied to the lobbyists, in so holding the court emphasized two limitations necessary to the statute's constitutionality: first, the national defense information must "necessarily be information which if disclosed, is potentially harmful to the United States," and second, "the defendant must

131. *Morison*, 844 F.2d at 1063 (citation omitted) (internal quotation marks omitted).

132. *Id.* at 1068–69 (quoting Branzburg v. Hayes, 408 U.S. 665, 691–92 (1972) (internal quotation marks omitted)).

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

134. *Id.* at 607–09.

135. *Id.* at 635–38.

136. *Id.* at 637.

know that disclosure of the information is potentially harmful to the United States."[137] The charges against Rosen and Weissman were eventually dropped because the government could not prove the requisite intent mandated by the court's interpretation of § 793.[138]

2. Case Law Interpreting § 798

Prosecutions under § 798 are extremely rare, and so, unsurprisingly, case law interpreting this statute is scant. Few courts have discussed § 798 in any meaningful way, and the Supreme Court has only mentioned the statute in passing.[139] In *United States v. Boyce*, the Ninth Circuit Court of Appeals held that under § 798 the "propriety of classification is irrelevant. The fact of classification of a document . . . is enough to satisfy the classification element of the offense."[140] However, a district court subsequently interpreting § 798 underscored the requirement that the government must classify the information for the statute to apply, noting that the information must be "specifically designated . . . for limited or restricted dissemination or distribution."[141]

IV. BALANCING FIRST AMENDMENT RIGHTS WITH THE GOVERNMENT'S INTEREST IN NATIONAL SECURITY

A. RESTRICTIONS OF THE PRESS AND THE FIRST AMENDMENT

The First Amendment of the U.S. Constitution states, "Congress shall make no law . . . abridging the freedom of speech, or of the press."[142] When a law restricts speech on the basis of its content—distinguishing favored speech from disfavored speech based on the ideas or views expressed therein—the restriction is subject to strict scrutiny, meaning the government must show that the challenged regulation is narrowly tailored

137. *Id.* at 641.

138. Jerry Markon, *U.S. Drops Case Against Ex-Lobbyists*, WASH. POST, May 2, 2009, at A1. *See also* SCHOENFELD, *supra* note 130, at 246–47.

139. *See* Snepp v. United States, 444 U.S. 507, 517 (1980) (Stevens, J., dissenting) (noting that Congress has enacted a number of criminal statutes, such as § 798, that punish the unauthorized dissemination of certain types of classified information); N.Y. Times Co. v. United States, 403 U.S. 713, 721 (1971) (Douglas, J., concurring) (arguing that § 793 does not apply to the press since other sections in the espionage statutes, such as § 798, specifically proscribe publication, and that therefore Congress "was capable of and did distinguish between publishing and communication in the various sections of the Espionage Act").

140. United States v. Boyce, 594 F.2d 1246, 1251 (9th Cir. 1979).

141. *In re* NSA Telecomm. Records Litig., 633 F. Supp. 2d 892, 908 (N.D. Cal. 2007).

142. U.S. CONST. amend. I.

to serve a compelling government interest.[143] So-called "content-based" restrictions are presumed invalid because they pose an inherent risk that the government seeks to suppress unpopular ideas or manipulate the public debate through coercion rather than advance a legitimate regulatory goal.[144]

Regulations unrelated to content are subject to an intermediate level of scrutiny, reflecting the less substantial risk of excising certain ideas or viewpoints from the public dialogue.[145] These "content-neutral" regulations may have an incidental effect on speech, but they are not intended to regulate speech based on its content.[146] Under the intermediate scrutiny standard, a content-neutral regulation is constitutional if it furthers an important or substantial governmental interest, the governmental interest is unrelated to the suppression of free expression, and the incidental restriction on any First Amendment freedoms is no greater than is essential to the furtherance of that interest.[147] In at least some cases, content-neutral regulations that are effectively naked prohibitions against pure speech must meet a more strict level of scrutiny to pass constitutional muster.[148]

A congressional act restricting the media implicates First Amendment concerns, but freedom of speech is not an absolute right.[149] The most often-cited example of unprotected speech is falsely shouting "fire" in a crowded room, causing panic.[150] Although the press ordinarily enjoys strong First Amendment protections when the published material at issue concerns a "matter of public significance,"[151] courts are highly deferential to the government when national security is at risk. Thus, there are extremely important interests involved on both sides of the balancing scale.

143. *See, e.g.*, United States v. Playboy Entm't Grp., Inc., 529 U.S. 803, 813 (2000) ("[I]f a statute regulates speech based on its content, it must be narrowly tailored to promote a compelling Government interest"); Sable Commc'ns v. FCC, 492 U.S. 115, 126 (1989) (same).

144. *See Playboy Entm't Grp.*, 529 U.S. at 812 ("Laws designed or intended to suppress or restrict the expression of specific speakers contradict basic First Amendment principles."); Turner Broad. Sys. v. FCC, 512 U.S. 622, 641 (1994) ("Laws [stifling speech on account of its message] pose the inherent risk that the Government seeks not to advance a legitimate regulatory goal, but to suppress unpopular ideas or information or manipulate the public debate through coercion rather than persuasion.").

145. *Turner Broad. Sys.*, 512 U.S. at 642.

146. *See* Ward v. Rock Against Racism, 491 U.S. 781, 791 (1989).

147. United States v. O'Brien, 391 U.S. 367, 377 (1968).

148. *See* Bartnicki v. Vopper, 532 U.S. 514, 526–27 (2001) (applying a strict level of scrutiny because the regulation of illegally intercepted conversations was "a naked prohibition against disclosures" and thus "fairly characterized as a regulation of pure speech").

149. Near v. Minnesota, 283 U.S. 697, 708 (1931).

150. Schenck v. United States, 249 U.S. 47, 52 (1919).

151. *See* Fla. Star v. B.J.F., 491 U.S. 524, 533 (1989) (citing Smith v. Daily Mail Publ'g Co., 443 U.S. 97, 103 (1979)) (declaring the name of a juvenile offender charged with murder to be a matter of public importance).

Since no courts have yet ruled on the constitutionality of the espionage statutes as applied to the media, this Note will address separately (1) the courts' traditional policy of deferring to the executive on matters related to national security and foreign policy; (2) how courts balance national security interests with First Amendment rights in the related context of prior restraint; and (3) criminal sanctions against the press in other contexts, concluding that these decisions leave open the possibility of prosecuting the media for unlawfully publishing national security information.

1. National Security and Foreign Policy

Courts are highly deferential to the executive when it comes to maintaining secrecy in the interests of national security and foreign policy.[152] Indeed, it is "'obvious and unarguable' that no governmental interest is more compelling than the security of the Nation."[153] In some cases, the Supreme Court has cited the Constitution as mandating that it defer to the executive in these matters.[154] Courts are especially sensitive to the need for secrecy in the intelligence community [155] given that intelligence operations depend on the ongoing maintenance of confidentiality.

a. Government Employees

Government employees enjoy fewer protections of their freedoms

152. *See* Haig v. Agee, 453 U.S. 280, 292 (1981) ("Matters intimately related to foreign policy and national security are rarely proper subjects for judicial intervention."); Harisiades v. Shaughnessy, 342 U.S. 580, 589 (1952) ("[P]olicies in regard to the conduct of foreign relations . . . are so exclusively entrusted to the political branches of government as to be largely immune from judicial inquiry or interference.").

153. *Haig*, 453 U.S. at 307 (quoting Aptheker v. Secretary of State, 378 U.S. 500, 509 (1964)). *Accord* Cole v. Young, 351 U.S. 536, 546 (1956); Zemel v. Rusk, 381 U.S. 1, 13–17 (1965).

154. *See* Chi. & S. Air Lines, Inc. v. Waterman Steamship Corp., 333 U.S. 103, 111 (1948) ("[T]he very nature of executive decisions as to foreign policy is political, not judicial. Such decisions are wholly confided by our Constitution to the political departments of the government, Executive, and Legislative. They are delicate, complex, and involve large elements of prophecy. They are and should be undertaken only by those directly responsible to the people whose welfare they advance or imperil. They are decisions of a kind for which the Judiciary has neither aptitude, facilities nor responsibility and which has long been held to belong in the domain of political power not subject to judicial intrusion or inquiry.").

155. *See* Snepp v. United States, 444 U.S. 507, 509 n.3 (1980) (per curiam) ("The Government has a compelling interest in protecting both the secrecy of information important to our national security and the appearance of confidentiality so essential to the effective operation of our foreign intelligence service."); United States v. Nixon, 418 U.S. 683, 710 (1974) ("The President, both as Commander-in-Chief and as the Nation's organ for foreign affairs, has available intelligence services whose reports are not and ought not to be published to the world.") (quoting Chi. & S. Air Lines, Inc., 333 U.S. at 111).

when performing their public functions[156] because they are in a position of trust with the government.[157] Employees with access to classified information must also sign a nondisclosure agreement.[158] Thus, in *Snepp v. United States*, the Court held that the government could require a former CIA agent to turn over a book he wrote about the Vietnam War for prepublication review, irrespective of whether the book actually contained classified information.[159] Likewise, in *Haig v. Agee*, the Court permitted the revocation of a former CIA employee's U.S. passport on the grounds that his activities abroad were causing serious damage to the national security of the United States.[160] The former CIA employee had announced a "campaign to fight the United States CIA wherever it is operating" and "to expose CIA officers and agents and to take the measures necessary to drive them out of the countries where they are operating."[161] Deferring to the executive branch, the Court noted Congress's recognition of "Executive authority to withhold passports on the basis of substantial reasons of national security and foreign policy"[162] and held that the former employee's claims concerning the First Amendment were without merit.[163]

b. Public Access to Information Regarding Intelligence Sources and Methods

Courts have consistently recognized that the governmental interest in protecting intelligence-gathering sources and methods outweighs the public's interest in accessing this information under the Freedom of Information Act ("FOIA").[164] In *Central Intelligence Agency v. Sims*, the Supreme Court held that the CIA properly exercised its broad authority when it withheld the names of scientific researchers who had participated in a CIA-funded project.[165] The Court emphasized the importance of maintaining the confidentiality of intelligence sources, noting that such sources would refuse to share information with the CIA if they believed the Agency could not maintain confidentiality, which could have a

156. *See* Garcetti v. Ceballos, 547 U.S. 410, 418 (2006) ("[W]hen a citizen enters government service the citizen by necessity must accept certain limitations on his or her freedom.").

157. *See Snepp*, 444 U.S. at 510–11 (discussing the "trust relationship" that arose from a citizen's employment with the CIA).

158. *See supra* Part III.A.

159. *Snepp*, 444 U.S. at 511.

160. Haig v. Agee, 453 U.S. 280, 309 (1981).

161. *Id.* at 283 (internal quotation marks omitted).

162. *Id.* at 293.

163. *Id.* at 306.

164. *See* Pub. L. No. 89-554, 80 Stat. 383 (1966) (codified as amended at 5 U.S.C. § 552 (2009)).

165. Cent. Intelligence Agency v. Sims, 471 U.S. 159, 181 (1985).

"devastating impact on the Agency's ability to carry out its mission."[166] The Court summarized the imperative of protecting intelligence sources and methods:

> Foreign intelligence services have both the capacity to gather and analyze any information that is in the public domain and the substantial expertise in deducing the identities of intelligence sources from seemingly unimportant details. . . . Accordingly, [the CIA] has power to withhold superficially innocuous information on the ground that it might enable an observer to discover the identity of an intelligence source.[167]

Cases in the lower courts also illustrate this point. In *Halperin v. Central Intelligence Agency*, the Court of Appeals for the D.C. Circuit refused the plaintiff's demand that the CIA disclose rates and total fees paid to attorneys retained by the agency to perform legal services because the information could reveal covert activities that constitute intelligence methods.[168] The court noted that "each individual piece of intelligence information, much like a piece of jigsaw puzzle, may aid in piecing together other bits of information even when the individual piece is not of obvious importance in itself."[169] Thus, "[w]hen combined with other small leads, the amount of a legal fee could well prove useful for identifying a covert transaction."[170] Similarly, in *Salisbury v. United States*, the D.C. Circuit denied a reporter's demand for release of certain documents under the FOIA, emphasizing that the documents would reveal which channels of communication between the United States and Hanoi the CIA and FBI were monitoring and ultimately lead to the loss of an intelligence source.[171]

2. Prior Restraint of the Press

Courts are less deferential to the government's interest in protecting secrets when constitutional rights are implicated. In particular, First Amendment rights directly conflict with the government's interest in protecting secrets when freedom of speech is at stake.[172] A prior restraint of speech, as opposed to punishment subsequent to speech, is especially

166. *Id.* at 175.
167. *Id.* at 178.
168. Halperin v. Cent. Intelligence Agency, 629 F.2d 144, 146 (D.C. Cir. 1980).
169. *Id.* at 150.
170. *Id.*
171. Salisbury v. United States, 690 F.2d 966, 972–73 (D.C. Cir. 1982).
172. *See* N.Y. Times Co. v. United States, 403 U.S. 713, 748 (1971) (Burger, C.J., dissenting) ("In these cases, the imperative of a free and unfettered press comes into collision with another imperative, the effective functioning of a complex modern government and specifically the effective exercise of certain constitutional powers of the Executive.").

disfavored.[173] As the Supreme Court explained, prior restraints are

> the most serious and the least tolerable infringement on First Amendment rights. A criminal penalty . . . is subject to the whole panoply of protections afforded by deferring the impact of the judgment until all avenues of appellate review have been exhausted . . . .
>
> A prior restraint, by contrast and by definition, has an immediate and irreversible sanction. If it can be said that a threat of criminal or civil sanctions after publication "chills" speech, prior restraint "freezes" it at least for the time.[174]

Nevertheless, the Court has allowed prior restraints on the media when national security may be jeopardized, especially during a time of war when national security is critical.[175] In *Schenck v. United States*, the Court upheld the conviction of a Socialist Party leader for circulating anti-war pamphlets during World War I, noting that "[w]hen a nation is at war many things that might be said in time of peace are such a hindrance to its effort that their utterance will not be endured so long as men fight and that no Court could regard them as protected by any constitutional right."[176] In 1931, the Court reiterated the importance of prior restraints during a time of war in *Near v. Minnesota*: "No one would question but that a government might prevent actual obstruction to its recruiting service or the publication of the sailing dates of transports or the number and location of troops."[177]

Until its 1971 decision in *New York Times v. United States* (the "*Pentagon Papers Case*"), the Court did not have occasion to consider whether the government can constitutionally enjoin the media from publishing national security information outside the context of war.[178] The Court implicitly answered this question in the affirmative when it held in the *Pentagon Papers Case* that in order to do so, the government must meet

173. *See* Neb. Press Ass'n v. Stuart, 427 U.S. 539, 559 (1976).

174. *Id.*

175. *Compare* Schenck v. United States, 249 U.S. 47, 51–52 (1919) (upholding the defendant's conviction of espionage for circulating anti-war pamphlets during World War I), Frohwerk v. United States, 249 U.S. 204, 209–10 (1919) (upholding the conviction of two newspaper publishers for publishing articles that criticized the war), *and* Debs v. United States, 249 U.S. 211, 215 (1919) (upholding the conviction of a Socialist Party leader for his speech at a public assembly, noting that one purpose of the speech was to "oppose not only war in general but this war, and that the opposition was so expressed that its natural and intended effect would be to obstruct recruiting"), *with* Brandenburg v. Ohio, 395 U.S. 444, 448–49 (1969) (per curiam) (reversing the conviction of a Ku Klux Klan leader for making racist remarks during a rally because the remarks did not incite immediate, illegal action).

176. *Schenck*, 249 U.S. at 52.

177. Near v. Minnesota, 283 U.S. 697, 716 (1931) (reversing, however, an injunction against the publication of any "malicious, scandalous, and defamatory newspaper" because such an order amounted to suppression and "censorship" of speech).

178. N.Y. Times Co. v. United States, 403 U.S. 713 (1971) (per curiam).

a "heavy burden" to justify the prior restraint.[179]

a. The *Pentagon Papers* Decision

In the *Pentagon Papers Case*, the Court held that the government could not prevent the *New York Times* and *Washington Post* from publishing a classified report regarding the Vietnam War.[180] The report, known as the "Pentagon Papers," was commissioned by Secretary of Defense Robert McNamara and discussed the United States' involvement in Vietnam from 1945 to 1967.[181] In March 1971, the report was leaked to the *New York Times* by Daniel Ellsberg, a former associate at the Rand Corporation.[182] The *Times* carefully reviewed the Pentagon Papers for three months and ultimately decided to publish it in a ten-part series, noting that the report revealed much more information than what was already known by the public, and that because the study had ended in 1968, it disclosed history rather than current military operations.[183] The first installment was published on June 13, 1971.[184] Three days later, Ellsberg gave a copy of the Pentagon Papers to the *Washington Post*.[185] The government immediately sought to enjoin the newspapers from further publications in the Washington D.C. and New York district courts; the cases had already reached the U.S. Supreme Court by June 25.[186]

The Supreme Court ultimately held that the government failed to meet its "heavy burden of showing justification for the imposition of [a prior] restraint" against further publication of the Pentagon Papers.[187] A majority of the justices could not agree, however, on why the government failed to meet this heavy burden. Thus, each of the nine justices wrote a separate opinion, with six justices concurring and three dissenting. Four of the concurring justices provided varying tests for when a prior restraint might be appropriate. For example, Justice Stewart thought the government could enjoin the press from publishing national security information only where it

179. *Id.* at 714.
180. *Id.*
181. GEOFFREY R. STONE, PERILOUS TIMES: FREE SPEECH IN WARTIME 500 (2004).
182. *Id.* at 501–02.
183. *Id.* at 503.
184. *Id.*
185. *Id.* at 506. On June 16th, the *Times* announced that it would obey a court-ordered injunction against printing the Pentagon Papers; this allegedly infuriated Ellsberg, leading him to leak the report to the *Post*, "which was miserable at having been scooped by the *Times*." *Id.*
186. *Id.* at 509.
187. N.Y. Times Co. v. United States, 403 U.S. 713, 714 (1971) (per curiam) (quoting Org. for a Better Austin v. Keefe, 402 U.S. 415, 419 (1971)).

would "surely result in direct, immediate, and irreparable damage to our Nation or its people."[188] Justice Stewart also emphasized the significant national security implications involved: "[I]t is elementary that the successful conduct of international diplomacy . . . require[s] both confidentiality and secrecy. Other nations can hardly deal with this Nation in an atmosphere of mutual trust unless they can be assured that their confidences will be kept."[189]

Even though the government had not argued for criminal punishment of the *New York Times* or *Washington Post*, six of the nine justices entertained the possibility of criminal prosecution.[190] Justice White, joined by Justice Stewart, specifically mentioned § 798, stating that he "would have no difficulty in sustaining convictions under [this section] on facts that would not justify the intervention of equity and the imposition of a

188. *Id.* at 730 (Stewart, J., concurring). Justice Brennan stated that a prior restraint against publication should only be permissible if the government can prove that publication would "inevitably, directly, and immediately cause the occurrence of an event kindred to imperiling the safety of a transport already at sea." *Id.* at 726–27 (Brennan, J., concurring). Justice White wrote that "the concededly extraordinary protection against prior restraints enjoyed by the press under our constitutional system" is not overcome even by a showing that the "revelation of . . . documents will do substantial damage to public interests." *Id.* at 730–31 (White, J., concurring). Justices Black and Douglas concurred in the decision but argued that prior restraints against the press are never permissible. *Id.* at 717 (Black, J., concurring) ("[T]he press must be left free to publish news, whatever the source, without censorship, injunctions, or prior restraints."); *id.* at 720 (Douglas, J., concurring) (explaining that the First Amendment "leaves . . . no room for governmental restraint on the press").

189. *Id.* at 728 (Stewart, J., concurring).

190. *See id.* at 730 (Stewart, J., concurring) ("Undoubtedly Congress has the power to enact specific and appropriate criminal laws to protect government property and preserve government secrets. Congress has passed such laws, and several of them are of very colorable relevance to the apparent circumstances of these cases. And if a criminal prosecution is instituted, it will be the responsibility of the courts to decide the applicability of the criminal law under which the charge is brought."); *id.* at 740 (White, J., concurring) ("[Congress] has not . . . authorized the injunctive remedy against threatened publication. It has apparently been satisfied to rely on criminal sanctions and their deterrent effect on the responsible as well as the irresponsible press. I am not, of course, saying that either of these newspapers has yet committed a crime or that either would commit a crime if it published all the material now in its possession. That matter must await resolution in the context of a criminal proceeding if one is instituted by the United States."); *id.* at 744 (Marshall, J., concurring) ("Of course, at this stage this Court could not and cannot determine whether there has been a violation of a particular statute or decide the constitutionality of any statute."); *id.* at 751 (Burger, C.J., dissenting) ("To me it is hardly believable that a newspaper long regarded as a great institution in American life would fail to perform one of the basic and simple duties of every citizen with respect to the discovery or possession of stolen property or secret government documents. That duty, I had thought—perhaps naively—was to report forthwith, to responsible public officers. This duty rests on taxi drivers, Justices, and the New York Times."); *id.* at 754–55 (Harlan, J., dissenting). *See also* 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, 361 (1986) (noting that a number of the Justices had "volunteered readings of the espionage statutes in relation to hypothetical criminal proceedings against the publishers, reporters and information sources involved, even though such questions had not been briefed" (footnote omitted)).

prior restraint."[191] Thus, the *Pentagon Papers Case* indicates that the Court would likely permit criminal sanctions against the media for publishing national security information.

3. Criminal Sanctions Against the Press in Other Contexts

The distinction between prior restraint and postpublication criminal sanctions is significant, drawing on the theory deeply woven into our law that a free society prefers to punish the few who abuse rights of speech rather than prevent the speech beforehand.[192] As William Blackstone pointedly stated, "[e]very freeman has an undoubted right to lay what sentiments he pleases before the public: to forbid this, is to destroy the freedom of the press: but if he publishes what is improper, mischievous, or illegal, he must take the consequence of his own temerity."[193]

Although the U.S. Supreme Court has not yet ruled on the constitutionality of a criminal prosecution of the press for publishing unlawfully leaked national security information, the Court has been careful to craft its holdings in other contexts so as not to foreclose the possibility of criminal sanctions against the press in all circumstances.[194] For example, in *Cox Broadcasting Corp. v. Cohn*, the Court declined to address "the broader question whether truthful publications may ever be subjected to civil or criminal liability consistently with the First . . . Amendment[]," holding only that a state may not impose sanctions on the publication of a rape victim's name obtained from public records.[195] Similarly, in *Landmark Communications, Inc. v. Virginia*, the Court considered the constitutionality of a statute authorizing criminal sanctions against a newspaper for publishing confidential information regarding judicial misconduct proceedings.[196] The Court reiterated that the "narrow and limited question" before it was whether the First Amendment "permits the criminal punishment of third persons who are strangers to the inquiry, including the news media, for divulging or publishing truthful information regarding confidential proceedings" and not "the possible applicability of

191. *N.Y. Times Co.*, 403 U.S. at 737 (White, J., concurring).

192. Se. Promotions, Ltd. v. Conrad, 420 U.S. 546, 559 (1975). The Court also made note of this in *Near v. Minnesota*, stating that the chief purpose of freedom of the press is "to prevent previous restraints upon publication." *Near*, 283 U.S. 697, 713 (1931).

193. 4 WILLIAM BLACKSTONE, COMMENTARIES *151–52.

194. *See* Bartnicki v. Vopper, 532 U.S. 514, 525 (2001); Fla. Star v. B.J.F., 491 U.S. 524, 536 (1989); Smith v. Daily Mail Publ'g Co., 443 U.S. 97, 105–06 (1979); Landmark Commc'ns v. Virginia, 435 U.S. 829, 837 (1978); Cox Broad. Co. v. Cohn, 420 U.S. 469, 492 (1975).

195. *Cox Broad. Corp.*, 420 U.S. at 491.

196. *Landmark Commc'ns*, 435 U.S. at 830.

the statute to one who secures the information by illegal means and thereafter divulges it."[197]

In *Smith v. Daily Mail Publishing Co.* ("*Daily Mail*"), the Court held that a state statute criminalizing the publication of an alleged juvenile delinquent's name violated the First Amendment where the name was obtained by the media lawfully.[198] The Court relied heavily on *Cox* and *Landmark*, noting that these cases "suggest strongly that if a newspaper lawfully obtains truthful information about a matter of public significance then state officials may not constitutionally punish publication of the information, absent a need to further a state interest of the highest order."[199] The Court again addressed this issue in *Florida Star v. B.J.F.*, similarly holding that a rape victim could not recover damages from a newspaper that had published the victim's name in violation of state law.[200] Unlike in *Cox*, the newspaper in *Florida Star* did not obtain the victim's name from public records; rather, the local sheriff's department had placed an incident report revealing the victim's name in its pressroom, where the newspaper retrieved it.[201] The Court reiterated the *Daily Mail* principle that "if a newspaper lawfully obtains truthful information about a matter of public significance then the state may not constitutionally punish publication of the information, absent a need to further a state interest of the highest order."[202]

In 2001, the Court applied the *Daily Mail* principle in *Bartnicki v. Vopper*, holding that the civil damages provision of a wiretap statute could not constitutionally prevent the broadcast of an illegally-intercepted telephone conversation by a radio station.[203] In *Bartnicki*, an unknown person intercepted and recorded a cellular phone conversation between two Pennsylvania teachers' union officials discussing failed negotiations with the school board.[204] The tape recording was anonymously left in the mailbox of the local citizens group's chairman.[205] The chairman passed it

197. *Id.* at 837.

198. *Daily Mail*, 443 U.S. at 105–06.

199. *Id.* at 103.

200. Fla. Star v. B.J.F., 491 U.S. 524, 541 (1989).

201. *Id.* at 527.

202. *Id.* at 533 (quoting *Daily Mail*, 443 U.S. at 103 (1979)).

203. Bartnicki v. Vopper, 532 U.S. 514, 527–28, 535 (2001).

204. *Id.* at 517–18. At one point in the conversation, one official referred to the strained negotiations with the school board, threatening, "[i]f they're not gonna move for three percent, we're gonna have to go to their, their homes . . . . To blow off their front porches, we'll have to do some work on some of those guys . . . . Really, uh, really and truthfully because this is, you know, this is bad news." *Id.* at 518–19.

205. *Id.* at 519.

on to a radio host, Frederick Vopper, who played it on his public affairs show.[206]

The federal statute at issue in *Bartnicki* purports to impose civil and criminal liability on any person who "intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of [the statute]."[207] Relying on this federal statutory provision as well as a similar state statute, the two union officials sought damages from the radio station and Vopper, alleging that the phone conversation was illegally intercepted and that the defendants violated the statutes by disclosing the contents of the communication that they knew or had reason to know was illegally intercepted.[208] The Third Circuit determined that the federal and state wiretapping statutes were "content neutral" laws properly subject to intermediate scrutiny under the First Amendment but held that the statutes were unconstitutional as applied in the *Bartnicki* case "because they deterred significantly more speech than necessary to protect the privacy interests at stake."[209]

The Supreme Court affirmed the Third Circuit but applied a higher level of scrutiny based on the *Daily Mail* principle. In doing so, the Court agreed with the Third Circuit that the statutes are "content-neutral law[s] of general applicability" but nevertheless held that their "naked prohibition against disclosures is fairly characterized as a regulation of pure speech."[210] Accordingly, the Court addressed what it described as a "narrower version" of a question raised but not resolved in the *Pentagon Papers Case* and in *Florida Star*: "whether, in cases where information has been acquired *unlawfully* by a newspaper or by a source, government may ever punish not only the unlawful acquisition but the ensuing publication as well."[211]

In defense of the statute's constitutionality, the government identified two interests served by criminally punishing those who disseminate lawfully obtained information when the source acquired it unlawfully—"first, the interest in removing an incentive for parties to intercept private conversations, and second, the interest in minimizing the harm to persons

206. *Id.*
207. 18 U.S.C. § 2511(1)(c) (2006).
208. *Bartnicki*, 532 U.S. at 519–20.
209. *Id.* at 521–22.
210. *Id.* at 526.
211. *Id.* at 528 (quoting Fla. Star v. B.J.F., 491 U.S. 524, 535 n.8 (1989)).

whose conversations have been illegally intercepted."[212] The Court dismissed the first interest, noting that it "would be quite remarkable to hold that speech by a law-abiding possessor of information can be suppressed in order to deter conduct by a non-law-abiding third party."[213] The Court gave the second interest more weight, noting that the privacy of communication is essential in a democratic society. Nevertheless, the Court concluded that "[i]n these cases, privacy concerns give way . . . [to] the interest in publishing matters of public importance."[214] Therefore, in *Bartnicki*, the government could not overcome its heavy burden of showing a need of the highest order.

In a separate concurring opinion, Justice Breyer, joined by Justice O'Connor, reiterated the limitation of the Court's holding to the particular facts in *Bartnicki*, stating that

> the Court does not create a "public interest" exception that swallows up the statutes' privacy-protecting general rule. Rather, it finds constitutional protection for publication of intercepted information of a special kind. Here, the speakers' legitimate privacy expectations are unusually low, and the public interest in defeating those expectations is unusually high. Given these circumstances, along with the lawful nature of respondents' behavior, the statutes' enforcement would disproportionately harm media freedom.[215]

Chief Justice Rehnquist, joined by Justice Scalia and Justice Thomas, dissented, arguing that the Court incorrectly applied strict scrutiny to a law that regulates speech irrespective of its content.[216]

In sum, the Supreme Court has persistently limited its holdings to the facts of each case, thereby reserving the possibility of enjoining the media from publishing national security information and applying appropriate criminal sanctions under the espionage statutes when the nation's security is at stake.

V. APPLYING THE CURRENT STATUTORY FRAMEWORK TO THE NEW MEDIA

As discussed in Part III.B.3, human intelligence is a vital source of the United States' intelligence operations abroad. By publishing information that reveals human intelligence sources, WikiLeaks has served very little

212. *Id.* at 529.
213. *Id.* at 529–30.
214. *Id.* at 534.
215. *Id.* at 540 (Breyer, J., concurring).
216. *Id.* at 544 (Rehnquist, C.J., dissenting).

public benefit while posing a grave risk to national security. The most immediate and tragic risk is the safety of informants and other civilians who share information with the U.S. government. By publishing information that identifies these individuals, WikiLeaks has placed their lives in danger. Additionally, publishing information about ongoing intelligence operations stifles diplomatic discussions, making it difficult to find individuals willing to share information with the U.S. government. As a former British diplomat explains,

> It is very difficult to conduct diplomacy effectively when your confidential deliberations are made public in this way. Mutual trust is the basis of such relations and once that trust is breached, candid conversations are less likely. It is like having a conversation in the pub with your best mate about problems with your girlfriend and then finding the content, possibly with a bit of spin added, posted on the internet. You won't be having that conversation again any time soon. And yet, unlike the conversation in the pub, governments do have to talk to each other, and being able to talk to each other frankly in private is essential to preserving their country's security and promoting its prosperity.[217]

Further, even when sources and informants continue to share information with the United States, U.S. agents will likely become more cautious in their reporting, censoring information that they fear could be plastered on the Internet. Unfortunately, this will likely cause the United States' intelligence operations to revert back to pre-9/11 "stovepipes" when agencies shared less information with each other.[218] Indeed, in response to Cablegate, the State Department completely disconnected its database from SIPRNet.[219]

Even the publication of a document that may not appear on its face to implicate methods or sources of intelligence gathering can damage the United States' national security interests by providing insights into patterns

217. Jonathan Powell, *US Embassy Cables: Leaks Happen. But on this Industrial Scale, Whose Interests Are Served?*, THE GUARDIAN (U.K.) (Nov. 29, 2010), http://www.guardian.co.uk/commentisfree/2010/nov/30/us-embassy-cables-wikileaks-public-interest.

218. *See* Kimery, *supra* note 25; Joseph I. Lieberman & Susan M. Collins, *How to Prevent the Next WikiLeaks Dump*, WALL ST. J., Jan. 13, 2011, at A17, *available at* http://online.wsj.com/article/SB10001424052748703779704576074340363346676.html; Dan Murphy, *How WikiLeaks Could Undo Post-9/11 Intelligence Reforms*, CHRISTIAN SCI. MONITOR (Nov. 30, 2010), http://www.csmonitor.com/World/Middle-East/2010/1130/How-WikiLeaks-could-undo-post-9-11-intelligence-reforms.

219. Massimo Calabresi, *State Pulls the Plug on SIPRNet*, TIME (Nov. 29, 2010), http://swampland.blogs.time.com/2010/11/29/state-pulls-the-plug-on-siprnet/.

of behavior, tactics, techniques and procedures.[220] This makes it impracticable for someone outside the government to sufficiently censor material: a responsible member of the press could spend months pouring over a set of documents to ensure that they do not reveal sources or methods of intelligence gathering and yet may still unknowingly compromise an ongoing intelligence operation. The Supreme Court has recognized that the media cannot properly judge what information is potentially harmful or dangerous:

> Predictive judgment . . . must be made by those with the necessary expertise in protecting classified information . . . . [I]t is not reasonably possible for an outside nonexpert body to review the substance of such a judgment . . . . Nor can such a body determine what constitutes an acceptable margin of error in assessing the potential risk.[221]

The Pentagon recently announced new measures to protect against internal leaks, such as preventing SIPRNet users from copying classified material onto removable devices and requiring two users to approve the transfer of data from a higher classification system to a lower classification system.[222] Changes have also been implemented to the classification system to expand declassification procedures.[223] Even with secure technology and strict document classification policies, however, there will always be a risk that someone with access to classified information will release it, whether inadvertently, purposefully with good intentions, or purposefully with intent to harm the United States.[224]

The context in which today's leaks take place intensifies this problem. WikiLeaks' publication of hundreds of thousands of classified documents demonstrates the power of technology—anyone with an Internet connection can quickly disseminate classified information to the entire world. As Kenneth Wainstein testified before Congress in December 2010,

> [WikiLeaks] arose over the past few years with the development of Internet technology that allows loose, virtual organizations to ferret out government secrets and disclose them in the unconstrained environment of cyberspace with little or no regard to our national security. And, it is a

220. *See* Coghlan & Whittell, *supra* note 39; *supra* notes 42–44 and accompanying text.

221. Navy v. Egan, 484 U.S. 518, 529 (1988).

222. Calabresi, *supra* note 219; Ellen Nakashima, *With Better Sharing of Data Comes Danger*, WASH. POST, Nov. 29, 2010, at A4, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2010/11/28/AR2010112804138.html.

223. *See supra* note 84 and accompanying text.

224. *See* PHILIP H. MELANSON, SECRECY WARS: NATIONAL SECURITY, PRIVACY, AND THE PUBLIC'S RIGHT TO KNOW 163 (2001) (describing the governmental security system as one in which leaks are inevitable).

> threat that will only get more dangerous with the advance of enabling technology and with the realization after these recent leaks that it takes so little to strike such a grandiose blow against government secrecy—nothing more than a computer, access to a disaffected government employee with a clearance, and a willingness to compromise our nation's interests and security.[225]

Publication of national security information may serve the public interest by providing citizens with insight into the inner workings of government, but the publication of some secret information poses a significant enough threat to the national security that the public interest is better served by keeping it secret.[226] Thus, Congress saw fit to protect against the publication of classified communications intelligence information without requiring that the government demonstrate a risk of harm because this information is uniquely "vital and vulnerable."[227]

Publication of information that reveals human intelligence sources is also particularly damaging because it not only destroys the source's usefulness, but also often places human lives at risk. In November 2010, WikiLeaks began publishing a cache of U.S. State Department cables, some of which revealed human intelligence sources.[228] By way of example, this Note will consider two possible remedies currently available to the United States: first, whether the government could prevent further publication with a court-ordered injunction, and second, the likelihood that a court would criminally sanction WikiLeaks under the espionage statutes.[229] As the following discussion will show, under the current statutory framework the government would likely be unable to successfully pursue either method for combatting the publication of information revealing human intelligences sources.

A. PRIOR RESTRAINT

The *Pentagon Papers Case* makes it clear that a court will only enjoin the publication of national security information if the government can meet

225. *Espionage Act and the Legal and Constitutional Issues Raised by Wikileaks: Hearing Before the H. Comm. on the Judiciary*, *supra* note 126, at 42–43 (statement of Kenneth L. Wainstein, Partner, O'Melveny & Myers LLP).

226. ELSEA, *supra* note 124, at 9.

227. *See supra* note 113 and accompanying text.

228. *See supra* Part II.A.4.

229. Other possible remedies this Note does not consider are theft of government property or receipt of stolen government property. *See* 18 U.S.C. § 641 (2006) (punishing both the theft and receipt of records or anything else of value belonging to the United States with a fine or imprisonment).

its "heavy burden" of showing justification for the prior restraint.[230] Although WikiLeaks has already published many (if not most) of the classified documents in its possession, it has yet to publish portions of the State Department cables. Thus, the government could seek a court order enjoining the website from releasing the remaining portions of these classified documents.

Because a court would review the request for an injunction in light of the *Pentagon Papers Case*, it is helpful to identify three key factors that distinguish that case from Cablegate, making it more probable that a court would approve the injunction. First, the Pentagon Papers was a backward-looking assessment of the United States' involvement in Vietnam. The report did not reveal any ongoing military or intelligence operations. Cablegate, on the other hand, contains over 100,000 classified State Department cables. Some of the released cables were as recent as six months old and others name intelligence sources and other individuals who have shared information with the United States. Second, although the *New York Times* and *Washington Post* did not reveal Daniel Ellsberg's identity when they began publishing the Pentagon Papers, the newspapers did not take active steps to protect his anonymity. WikiLeaks not only promises anonymity to those who leak classified information to its website, but also takes significant steps to ensure its sources' identities cannot be discovered by protecting the information in its possession with "cutting-edge cryptographic information technologies."[231] Finally, the amount of documents WikiLeaks has published is staggering, suggesting that WikiLeaks aims to stir controversy at the expense of the United States rather than apprise the international public of important information regarding its governments.

Although an injunction against WikiLeaks prohibiting further release of the State Department cables may be legally tenable, such an injunction would not be practically effective against WikiLeaks and other new media outlets. The efficacy of an injunction completely depends upon the publisher honoring it. New media outlets such as WikiLeaks operate on multiple servers in different countries—their whereabouts often unknown—making it easy to simply transfer the material to different servers, thereby rendering an injunction ineffective.[232] Even more

230. *See* N.Y. Times Co. v. United States, 403 U.S. 713, 714 (1971) (because an injunction prohibiting the release of classified information was a prior restraint, the government had a heavy burden justifying such action); *supra* Part IV.A.2.a.

231. *What is Wikileaks?*, *supra* note 13.

232. In 2008, a U.S. court ordered a domestic Internet Service Provider ("ISP") to shut down

significantly, WikiLeaks' threat to release an "insurance file" if its website is shut down clearly demonstrates it would not respect an injunction.[233] WikiLeaks' threat places governments in a very unfortunate dilemma: do nothing, or seek an injunction and risk the release of additional uncensored documents, causing even greater risk to the national security and the lives of intelligence sources and informants.

Finally, an injunction may not deter future leaks by new media outlets such as WikiLeaks because it would not result in any personal consequences for the individuals operating the website, whereas a criminal warrant could lead to the extradition and prosecution of those who operate the offending website.[234]

B. CRIMINAL SANCTIONS

Given that a prior restraint against new media outlets such as WikiLeaks would likely not be effective, the criminal law is the government's best possible remedy. Although postpublication criminal sanctions only operate after the leak has occurred, they can deter future leaks by those who are prosecuted and prevent copycat operations from surfacing. Under the current statutory framework, a prosecution against WikiLeaks for publishing information revealing human intelligence sources would only be possible under § 793(e) of the Espionage Act. Section 793(e) proscribes the communication of NDI by persons with unlawful possession of the information if the individual communicating it has reason to believe the information could be used to the injury of the United States or to the advantage of any foreign nation.[235]

A criminal prosecution against WikiLeaks would no doubt face a First Amendment challenge, but the *AIPAC Case* indicates that this challenge would probably not survive.[236] Although the district court's conclusion in

WikiLeaks after the website posted documents from Julius Baer Bank and Trust. Adam Liptak & Brad Stone, *Judge Shuts Down Web Site Specializing in Leaks*, N.Y. TIMES, Feb. 20, 2008, at A14. Although the ISP complied with the order, WikiLeaks remained accessible through multiple mirror sites located in other countries. Meier, *supra* note 6, at 204. *See also* Davidson, *supra* note 5, at 84 ("WikiLeaks' design would almost certainly negate most if not all external attempts at containing its content. Attempts at enforcement would thus seem to start a digital game of whack-a-mole, with an injunction against one WikiLeaks site simply leading to the posting by another WikiLeaks site, and on and on.").

233. *See supra* note 15 and accompanying text.

234. While there is no general rule of international law that requires a foreign state to surrender an offender, the United States has bilateral extradition treaties to facilitate extradition. *See* ILIAS BANTEKAS, SUSAN NASH & MARK MACKAREL, INTERNATIONAL CRIMINAL LAW 139 (2001).

235. 18 U.S.C. § 793(e) (2006). *See also supra* text accompanying notes 102–04.

236. *See supra* text accompanying notes 133–37.

the *AIPAC Case* is not binding precedent, higher courts would likely rely heavily on its thorough analysis to conclude that the government can punish those outside the government for the unauthorized publication of NDI.[237]

While some have argued that *Bartnicki* forecloses the possibility of a successful criminal prosecution against the media in the context of national security,[238] a prosecution of WikiLeaks would probably not be bound by that decision because it involved different, less compelling interests. The privacy interests implicated in *Bartnicki* were strong, but they are not nearly as compelling as the government's interest in protecting national security, particularly when the publisher has revealed sensitive intelligence sources. Several courts have recognized the compelling government interest in protecting sources and methods of intelligence gathering,[239] and the Supreme Court has declared that "no governmental interest is more compelling than the security of the Nation."[240] Even the *Bartnicki* Court made clear that its holding was limited to the facts of that case.[241]

Additionally, WikiLeaks promises its sources anonymity and uses cutting-edge technology to fulfill this promise. In *Bartnicki*, on the other hand, the radio station neither solicited the unlawfully obtained information, nor did it actively protect the source's anonymity. Further, in *Bartnicki*, the radio station's receipt of an unlawfully recorded conversation was not proscribed by the statute, whereas the Espionage Act explicitly prohibits the receipt of NDI by a person with knowledge 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.[242] The Cablegate documents include classified information, some of which display additional warnings and markings indicating that the contents are extremely sensitive. Thus, a court reviewing a prosecution of WikiLeaks under § 793(e) would likely not find *Bartnicki* to be dispositive.

237. *See* SCHOENFELD, *supra* note 130, at 249 (arguing that the district court judge presiding over the *AIPAC Case* explicated the law so well that higher courts would likely rely on his reasoning).

238. *See* Laura E. Zirkle, Case Note, Bartnicki v. Vopper, *A Public Concern Exception for the Press and Its Disclosure of Unlawfully Obtained Information*, 11 GEO. MASON L. REV. 441, 459 (2002) ("In light of the public concern exception articulated in Bartnicki, . . . the Court would likely elect not to punish the press for its unlawful disclosure of [classified] information, upon balancing the desire to inform the public during such a critical period [in the war on terror] against the need to preserve the secrecy of the information.").

239. *See supra* Part IV.A.1.

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

241. Bartnicki v. Vopper, 532 U.S. 514, 528–29 (2001).

242. 18 U.S.C. § 793(c) (2006).

Despite overcoming the First Amendment hurdle in a prosecution against WikiLeaks, the government would face two serious, likely insurmountable, challenges under § 793. First, the government must prove that WikiLeaks had "reason to believe the [State Department cables] could be used to the injury of the United States or to the advantage of any foreign nation."[243] The government could argue that this purpose can be inferred from WikiLeaks' above-mentioned behavior. This would be a novel argument, but given the nature of WikiLeaks' actions a court might entertain it. Since the statute covers a broad range of national security information, however, a court would probably be less deferential to the government's assertion that WikiLeaks was effectively on notice that publication of Cablegate posed a risk of injury to the United States. Second, even if the government can overcome its burden of proving WikiLeaks had the requisite intent, § 793 would not apply to many of the State Department cables since they may not constitute "information related to the national defense."[244] Thus, under the current statutory framework the government is largely unable to prevent the publication of information revealing human intelligences sources.

VI. CONGRESS MUST ENACT LEGISLATION SPECIFICALLY DESIGNED TO PROTECT HUMAN INTELLIGENCE SOURCES

As this Note has demonstrated, there is a gap in the current espionage statutes such that the unlawful publication of classified human intelligence information is only punishable if the government can prove that the information is "related to the national defense" and that the publisher had the requisite intent—namely, "reason to believe [it] could be used to the injury of the United States or to the advantage of any foreign nation."[245] The vulnerability of human intelligence sources and the ease with which classified information can be published by new media outlets such as WikiLeaks dictate that Congress must amend the espionage statutes to better protect this source of information.[246] An amendment must be carefully drafted, however, to strike a proper balance between the

243. *See id.* § 793(e).

244. *See supra* Part II.A.

245. 18 U.S.C. § 793(e).

246. Some commentators have similarly argued that the Intelligence Identities Protection Act ("IIPA") should be amended to better protect intelligence sources. *See, e.g.*, Andrew M. Szilagyi, Note, *Blowing Its Cover: How the Intelligence Identities Protection Act Has Masqueraded as an Effective Law and Why It Must Be Amended*, 51 WM. & MARY L. REV. 2269, 2274 (2010) (arguing that the IIPA must be amended to "effectively serve its purpose and avoid becoming completely defunct").

government's interest in protecting national security and the individual rights protected by the First Amendment. The legislature must enact "clear, precise and extremely limited prohibitions on the . . . disclosure of only the most necessary of secrets."[247]

The proposed SHIELD Act responds to the gap in the espionage statutes by amending § 798 to protect against the publication of information revealing human intelligence sources. If enacted, the SHIELD Act will permit the prosecution of the media for knowingly and willfully publishing classified information "concerning the identity of a classified source or informant of an element of the intelligence community of the United States."[248] Unlike § 793 of the Espionage Act, § 798 already narrowly defines a class of protected information, the publication of which is punishable irrespective of the publisher's intent.

The narrow application of § 798 makes an amendment to this statute, as opposed to § 793, ideal for several reasons. First, there will be significantly less ambiguity over what type of information the statute covers. Section 798 specifically defines narrow categories of classified information, whereas § 793 broadly applies to "information related to the national defense." Second, the use of the term "publishes" in § 798 makes it clear that the statute is intended to bar public speech.[249] Third, because of the statute's narrow application, the government will not need to overcome the nearly impossible hurdle of proving that the offending publisher had "anti-American or pro-foreign motives."[250]

A. ESTABLISHING A WORKABLE ENFORCEMENT SCHEME

An amendment of the espionage statutes would be futile if the government fails to enforce it against those who illicitly leak and publish classified information. Historically, the government has forgone prosecution of publishers for revealing sensitive national security information.[251] One CIA veteran identified a systemic failure to enforce the espionage laws, citing a "lack of political will to deal firmly and consistently with unauthorized . . . leakers."[252] This lack of enforcement

247. Alan M. Dershowitz, *Who Needs to Know?*, N.Y. TIMES, May 30, 2010, at BR13 (reviewing GABRIEL SCHOENFELD, NECESSARY SECRETS (2010)).

248. *See* SHIELD Act, S. 4004, 111th Cong. § 2(a) (2010). *See also supra* Part III.B.3.b.

249. Edgar & Schmidt, *supra* note 94, at 1065.

250. *See id.*

251. *See* SCHOENFELD, *supra* note 130, at 255–56 (noting that the government's failure to prosecute the *New York Times* for revealing the NSA wiretapping program may have led to the *Times*' subsequent publication of the SWIFT program).

252. James B. Bruce, *Law and Leaks of Classified Intelligence: The Consequences of Permissive*

has "perpetuate[d] the notion that the government can do nothing to stop leaks of classified information."[253] In order to effectively punish those who publish classified human intelligence information and deter such publication in the future, the government must establish a consistent enforcement scheme.

As noted in Part II, there are key differences between the traditional media and certain new media outlets such as WikiLeaks. Such differences indicate that a prosecution of these new media organizations would be far less politically problematic. At the very least, the government should prosecute WikiLeaks, which has both the means and purpose of undermining the United States' national security irrespective of whether its activities serve the public's interest. WikiLeaks' sole purpose is the collection and public release of secrets. Unlike traditional media outlets, WikiLeaks distributes troves of uncensored material instantaneously, demonstrating an extreme lack of concern for national security and for the safety of individuals named in the reports it releases. In the past, newspapers and other journalists have often sought and published government secrets for specific stories and have printed secrets that were delivered to them, but no journalist has matched WikiLeaks' open invitation to send it secret information.[254] "WikiLeaks' indiscriminate dumping of tens of thousands of purloined classified documents into the public domain for friend and foe to read is neither responsible journalism nor does it strike a blow for [government] transparency."[255]

Finally, there are currently serious allegations against the government for improperly classifying information that poses no risk to the national security.[256] Indeed, some who have reviewed the cache of classified

Neglect, 47 STUD. INTELLIGENCE 39, 44 (2003), *available at* https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol47no1/pdf/v47i1a04p.pdf.

253. *Presidential Directive on the Use of Polygraphs and Prepublication Review: Hearings Before the Subcomm. on Civil and Constitutional Rights of the Comm. on the Judiciary House of Representatives*, 98th Cong. app. 2 at 178 (1985) (Report of the Interdepartmental Group on Unauthorized Disclosures of Classified Information).

254. Pete Yost, *WikiLeaks: Espionage? Journalism? Something Else?*, HUFFINGTON POST (Nov. 30, 2010 7:53 PM), http://www.huffingtonpost.com/huff-wires/20101130/us-wikileaks-prosecution/.

255. John Hughes, *WikiLeaks' Real Victim: Old-School Code of Trust*, CHRISTIAN SCI. MONITOR (Dec. 14, 2010), http://www.csmonitor.com/Commentary/John-Hughes/2010/1214/WikiLeaks-real-victim-old-school-code-of-trust.

256. *See, e.g.*, *Espionage Act and the Legal and Constitutional Issues Raised by Wikileaks: Hearing Before the H. Comm. on the Judiciary*, *supra* note 126, at 22–23 (2010) (statement of Abbe David Lowell, Partner, McDermott Will & Emery LLP) (describing the problem of overclassification of government documents).

documents in Cablegate argue that it contains many examples of overclassification.[257] While the overclassification problem is beyond the scope of this Note, it is an integral part of the solution this Note proposes because it gives organizations like WikiLeaks an excuse to disregard the classification system. Thus, additional statutory protections against the unlawful publication of classified human intelligence information must be accompanied by responsible classification policies and practices enforced across all agencies.

VII. CONCLUSION

WikiLeaks has made it more apparent than ever that the paradigm of the media has shifted. By publishing the massive volume of State Department cables, WikiLeaks undermined the entire process of diplomacy, posing a substantial threat to the U.S. government's ability to protect the national security and risking the lives of individuals who share information with the United States. Criminal sanctions should be available to punish organizations like WikiLeaks when they indiscriminately publish classified information revealing human intelligence sources. The government must update its laws to effectively strike a proper balance between legitimate secrecy and the public's right to information about its government in the digital age.

257. *See* Julian Hattem, *WikiLeaks and the Classification Follies*, CTR. FOR PUBLIC INTEGRITY (Dec. 22, 2010, 5:30 PM), http://www.iwatchnews.org/2010/12/22/2239/wikileaks-and-classification-follies.