6-15-2011

The Publication of National Security Information in the Digital Age

Mary-Rose Papandrea
Boston College Law School, papandrm@bc.edu

Recommended Citation
Mary-Rose Papandrea. "The Publication of National Security Information in the Digital Age." *Journal of National Security Law & Policy* 5, no.1 (2011): 119-130.

The Publication of National Security Information in the Digital Age

Mary-Rose Papandrea*

In one of her speeches on Internet freedom, Secretary of State Hillary Rodham Clinton said that "[t]he fact that WikiLeaks used the internet is not the reason we criticized its actions."[1] Although Clinton is correct that it is essential to separate the technology WikiLeaks uses from its actions, the digital age has raised new concerns about the unauthorized dissemination of sensitive national security information. New technology has made it much easier to leak and otherwise disseminate national security information. At the same time, leaks continue to play an essential role in checking governmental power and often make invaluable contributions to our public debate. WikiLeaks has prompted renewed debate concerning when the disclosure of national security information by nongovernmental actors should be protected, both as a policy matter and as a matter of constitutional law.

One dominant theme in the discussion of how to strike the balance between an informed public and the need to protect legitimate national security secrets is whether new media entities like WikiLeaks are part of "the press" and whether Julian Assange and his cohorts are engaging in "journalism."[2] As the gathering and distribution of news and information becomes more widely dispersed, and the act of informing the public more participatory and collaborative, however, determining who is engaging in journalism and what constitutes the press has become increasingly difficult. It is not possible to draw lines based on the medium of communication, the journalistic background of the publisher, the editing process, the size of the audience, or the methods used to obtain the information.

* Associate Professor, Boston College Law School. The author thanks Noah C. N. Hampson for his invaluable research assistance.

1. Hillary Rodham Clinton, U.S. Sec'y of State, Internet Rights and Wrongs: Choices and Challenges in a Networked World, Address at George Washington University (Feb. 15, 2011), *available at* http://www.state.gov/secretary/rm/2011/02/156619.htm.

2. *See* Jonathan Peters, *WikiLeaks, the First Amendment, and the Press*, HARVARD LAW AND POLICY REVIEW, Apr. 18, 2011, *available at* http://hlpronline.com/2011/04/wikileaks-the-first-amendment-and-the-press/. For a thorough summary of the government's and mainstream media's disdain for WikiLeaks and Julian Assange, see Yochai Benckler, *A Free Irresponsible Press: WikiLeaks and the Battle Over the Soul of the Networked Fourth Estate*, HARV. C.R.-C.L. L. REV. (forthcoming 2011), *available at* http://www. benkler.org/Benkler_Wikileaks_current.pdf.

Rather than attempt to define who is a journalist or what is the press, Congress and courts should give careful consideration to the relevant scienter requirements that would apply in cases involving nongovernmental actors. In such cases, the relevant laws should require that the offender acted with a subjective intent to harm the United States or with reckless indifference to any such harm. Such a test provides a means of protecting those who disseminate national security information responsibly and with a good-faith purpose to inform the public debate. This intent requirement would be in addition to proof of imminent and serious harm to U.S. interests.[3]

I. THE IMPORTANCE OF LEAKS

Throughout our nation's history, democratic principles of open government have often clashed with the asserted need for secrecy in diplomatic and military affairs. The executive branch enjoys virtually unbridled authority to control the flow of national security information to the public. The primary means by which the executive branch exercises this power is the classification system.[4] The Freedom of Information Act (FOIA)[5] and whistleblower protection laws[6] are ineffective checks on this power. FOIA provides a cumbersome and limited mechanism for obtaining national security information.[7] Whistleblower protection laws can be confusing, and they provide minimal protection to employees who reveal national security information.[8] Although it might be possible to provide better statutory checks on executive classification authority, it is doubtful that any statutory fix could resolve the endemic problem of overclassification.[9]

As a result of the tension between the executive branch's asserted need for secrecy and the democratic requirements of openness and transparency, the government and the media have engaged in a game of leaks. Although

3. *See* Geoffrey R. Stone, *WikiLeaks, the Proposed SHIELD Act, and the First Amendment*, 5 J. NAT'L SECURITY L. & POL'Y 105 (2011).

4. For an excellent overview of the classification system and the problem of overclassification, see Heidi Kitrosser, *Classified Information Leaks and Free Speech*, U. ILL. L. REV. 881, 888-896 (2008).

5. 5 U.S.C. §552 (2006), *amended by* OPEN Government Act of 2007, Pub. L. No. 110-175, 121 Stat. 2524.

6. Intelligence Community Whistleblower Protection Act of 1998, Pub. L. No. 105-272, 112 Stat. 2413 (codified as amended at 50 U.S.C. §403(q) (2006)); Whistleblower Protection Act of 1989, Pub. L. No. 101-12, 103 Stat. 16 (codified as amended at 5 U.S.C. §2302 (2006)); Military Whistleblower Protection Act of 1988, Pub. L. No. 100-456, 102 Stat. 2027 (codified as amended at 10 U.S.C. §1034 (2006)).

7. Kitrosser, *supra* note 4, at 894.

8. *See* Mary-Rose Papandrea, *Lapdogs, Watchdogs, and Scapegoats: The Press and National Security Information*, 83 INDIANA L. J. 233, 246-248 (2008).

9. Kitrosser, *supra* note 4, at 896.

the media is often criticized for publishing national security information, its access to information frequently is the result of a planned strategy by a government official to advance or promote a particular policy, sabotage the plans or policies of rival agencies or political parties, discredit opponents, float a public opinion trial balloon, or expose corruption or illegal activities. Indeed, leaks have been part of this nation's history since its founding and are an important way in which government officials promote their agendas and attempt to persuade the public.[10] As the saying goes, the ship of state is the only known vessel that leaks from the top. Thus, it is important to keep in mind that the executive branch does not want to end all leaks; it simply wants to end the leaks that it does not like.[11] This is not to deny that some leaks come from self-styled patriots or disgruntled employees. Regardless of the motivation of the leaker, however, these leaks also can make valuable contributions to the public debate.

Leaks have played a key role in exposing illegal or morally reprehensible government practices, such as the treatment of prisoners in Abu Ghraib, extraordinary rendition, and the NSA warrantless wiretapping program. Relying on leaks is hardly a perfect way of making sure the public receives essential information or of checking excessive government power; it does not guarantee that improperly classified information will come to light, or that genuinely sensitive information will remain secret.[12] Nevertheless, this imperfect system is the best we have for checking the virtually unbridled power of the government to control the dissemination of national security information.

For at least the last century, it has generally been mainstream media outlets – especially the nation's leading newspapers – that have published sensitive national security information. For the most part, these entities have been both cooperative and responsible in their publication decisions. They routinely ask the government for guidance on the ramifications of the national security information in their possession and frequently have withheld stories or limited their scope in order to soften their impact. For example, at President Kennedy's request, *The New York Times* agreed to delay publishing a story about nuclear weapons in Cuba.[13] During the Iran

10. For a thorough discussion of the history of intentional, strategic leaks, see Papandrea, *supra* note 8, at 249-262.

11. *See* Tom Wicker, *Leak On, O Ship of State!*, N.Y. TIMES, Jan. 26, 1982, at A15; *see also* LEON V. SIGAL, REPORTERS AND OFFICIALS: THE ORGANIZATION AND POLITICS OF NEWSMAKING 145 (1973) (quoting aide to President Johnson as saying that "the people at 1600 Pennsylvania Avenue are not really worried about all leaks – only those that originate outside the White House").

12. *See* Louis Henkin, *The Right To Know and the Duty To Withhold: The Case of the Pentagon Papers*, 120 U. PA. L. REV. 271, 278 (1971).

13. MAX FRANKEL, HIGH NOON IN THE COLD WAR: KENNEDY, KHRUSHCHEV, AND THE CUBAN MISSILE CRISIS 108-110 (2004).

hostage crisis, the press withheld stories that might have harmed the hostages or undermined secret negotiations for their release.[14] In 1986, *The Washington Post* acceded to the White House's request to refrain from publishing information about an underwater spy project in Russian waters called "Ivy Bells."[15] Famed journalist Benjamin Bradlee has said that while he was editor at the *Post*, he "kept many stories out of the paper because I felt – without any government pressure – that the national security would be harmed by their publication."[16] More recently, the *Times* sat on its NSA wiretapping story for a year while government officials argued for the necessity of keeping the program secret.[17] Similarly, when the *Post* published an article revealing the existence of "black sites," where terrorist suspects were secretly detained and interrogated[18] it agreed to the government's request to withhold the names of the Eastern European countries that were participating in the program. To be sure, the government has not always agreed with the publication decisions of the mainstream media. But newspapers and other news outlets in possession of national security information have generally made a serious effort to take the administration's concerns seriously, and there is little evidence that any of their publication decisions have actually caused the United States serious harm.

For decades this country has lived in a state of "benign indeterminancy" regarding the constitutionality of prosecutions for the receipt and dissemination of national security information.[19] On the one hand, this state of affairs has served us well. Major media outlets generally have been responsible in exercising a "gate-keeping" function, disseminating sensitive national security information only when the benefits of that dissemination outweigh the harm. If anything, there has been more concern that the established press has not been as willing as new media to challenge government orthodoxy.[20] On the other hand, we cannot assume that all

14. DEBORAH HOLMES, GOVERNING THE PRESS: MEDIA FREEDOM IN THE U.S. AND GREAT BRITAIN 61-62 (1986).

15. Richard Zoglin, *Questions of National Security*, TIME, June 2, 1986, at 67.

16. BENJAMIN BRADLEE, A GOOD LIFE: NEWSPAPERING AND OTHER ADVENTURES 474 (1995).

17. James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES, Dec. 16, 2005, at A1.

18. Dana Priest, *CIA Holds Terror Suspects in Secret Prisons*, WASH. POST, Nov. 2, 2005, at A1.

19. Harold Edgar & Benno C. Schmidt, Jr., *The Espionage Act and Publication of Defense Information*, 73 COLUM. L. REV. 929, 936 (1973). *See also* William H. Freivogel, *Publishing National Security Secrets: The Case for Benign Indeterminacy*, 3 J. NAT'L SECURITY L. & POL'Y 95 (2010).

20. For a lengthier discussion of the failures of the mainstream media in recent years, see Mary-Rose Papandrea, *Citizen Journalism and the Reporter's Privilege*, 91 MINN. L. REV. 515, 524-528 (2007).

journalists – whether professional or belonging to the new "citizen media" class – will continue to act responsibly.

II. NEW CHALLENGES

The evolution of the Internet and the dispersal of the newsgathering and dissemination functions traditionally exercised by major media outlets have the potential to undermine this system of leaks that has been working rather well since the development of mass media over a century ago.

Prior to the Internet, those in possession of national security information who wanted to reveal it to the public had to go through a traditional media outlet to accomplish that goal. Thus, when Daniel Ellsberg was in possession of the Pentagon Papers, he went to several major newspapers as well as the three major television networks in an effort to find an outlet.[21] Today's leakers can deposit a treasure trove of information on any number of websites around the world designed to receive confidential information. Admittedly, Julian Assange of WikiLeaks cooperated with some of the world's most influential newspapers in order to assure that the information he had collected would be noticed. Nevertheless, the government has good reason to be concerned that its enemies will not limit their reading to *The New York Times* and *The Washington Post* and instead will be searching the Internet for valuable information. The Internet makes it easy to search vast databases with little effort.

The government has never prosecuted the press for publishing national security information and has instead traditionally pursued the government employees or contractors who leaked the information in the first place.[22] Although the government has arrested Bradley Manning, the person identified as primarily responsible for the leak of U.S. classified information to WikiLeaks, it may not be so easy to identify leakers in the future. Technology has developed to make it possible for individuals to exchange information anonymously, making it impossible for the

21. DAVID RUDENSTINE, THE DAY THE PRESSES STOPPED: THE STORY OF THE PENTAGON PAPERS CASE 127, 248 (1998). Unlike the major newspapers, the networks were unwilling to publish the Pentagon Papers because they feared retaliation from the Federal Communications Commission. *Id*. at 127.

22. *See* Scott Shane, *Obama Takes a Hard Line Against Leaks to Press*, N.Y. TIMES, June 12, 2010, at A1, *available at* https://www.nytimes.com/2010/06/12/us/politics/12 leak.html. From time to time the government has also subpoenaed reporters to obtain the identity of individuals who leaked classified information. *See, e.g*., Adam Liptak & Maria Newman, *New York Times Reporter Jailed for Keeping Source Secret*, N.Y. TIMES, July 6, 2005 (describing subpoenas for identities of confidential sources to reporters Matt Cooper and Judith Miller, and Miller's being jailed for contempt of court for her refusal to comply), *available at* https://www.nytimes.com/2005/07/06/politics/06cnd-leak.html?_r=1&page wanted=2.

government to subpoena the identity of leakers from the website that received the information. Technology has given rise to the development of intermediaries like WikiLeaks that can serve as a conduit of information between the original sources and the public. As Jay Rosen has noted, sources no longer have to meet a reporter in a dark parking garage.[23]

Although new technology threatens the old way of doing things, we have to keep in mind that the traditional media outlets do not have a monopoly on the ability to inform the public in a responsible way. Non-professional journalists have provided valuable information to the public debate that the mainstream media either missed or ignored.[24] WikiLeaks itself has uncovered valuable information about human rights abuses and other atrocities in countries around the globe; in fact, in 2009, WikiLeaks won an award from Amnesty International for its release of documents concerning the extra-judicial killings and disappearances in Kenya.[25] Rather than condemning non-traditional media websites, we need to begin to recognize that new technology allows non-professionals to play an important role in informing the public.

One common justification for distinguishing WikiLeaks from the traditional media is that it does not engage in the traditional journalistic practice of carefully analyzing and giving context to the material that it publishes.[26] As a factual matter, it is inaccurate to argue that WikiLeaks does not engage in any editorial practices. Although initially WikiLeaks did not filter the electronic files it obtained, it no longer simply publishes every bit of information it receives.[27] In addition, it has sought government guidance on what names and identifying information it should redact from its materials in order to avoid a significant risk of harm to individuals.[28] Furthermore, regardless of how WikiLeaks itself operates, it certainly is not

23. Jay Rosen, *Jay Rosen on WikiLeaks: "The Watchdog Press Died; We Have This Instead*," VIMEO, Dec. 2, 2010, http://vimeo.com/17393373?utm_source=www.twitter.com%2Fstkonrath&utm_medium=twitter&utm_campaign=future-of-journalism.

24. *See* Papandrea, *supra* note 20, at 524-528 (summarizing some of the contributions of bloggers and other online media outlets to the public discourse).

25. *See* Amnesty International, *Amnesty International Media Awards 2009: Winners and Shortlist* (2009), http://www.amnesty.org.uk/uploads/documents/doc_20539.pdf.

26. *See*, *e.g.*, David Rivkin & Bruce Brown, *Prosecute Assange with Espionage Act*, USA TODAY, Dec. 14, 2010, *available at* http://www.usatoday.com/news/opinion/forum/2010-12-15-column15_ST1_N.htm.

27. For a summary of the evolving modus operandi of WikiLeaks, see Yochai Benckler, *supra* note 2, at 4-14.

28. Letter from Julian Assange to U.S. Ambassador Louis B. Susman (Nov. 26, 2010), *available at* http://www.foreignpolicy.com/files/fp_uploaded_documents/101129_plugin-Letter-to-US-Ambassador-from-Julian-Assange-26-November-2010.pdf. State Department Legal Advisor Harold Koh wrote a stern letter to WikiLeaks flatly refusing to have any discussions about the sensitive material WikiLeaks possessed and demanding the immediate return of all documents that it possessed. Letter from Harold Hongju Koh to Jennifer Robinson, Attorney for Julian Assange (Nov. 27, 2010), *available at* http://media.washingtonpost.com/wp-srv/politics/documents/Dept_of_State_Assange_letter.pdf.

the case that every website would function in the same way. WikiLeaks was not the first website committed to transparency, and it is almost certainly not the last.[29]

It is also true that the traditional media is capable of making irresponsible publication decisions and publishing national security information without due care and consideration. Indeed, during the debates leading to the passage of the Espionage Act of 1917, Congress was concerned about "disloyal papers" that had loyalties to Germany or other enemies.[30] In 1973, long before the Internet was developed, Harold Edgar and Benno Schmidt noted in their seminal article on the Espionage Act that "some underground newspaper stands ready to publish anything that the Times deems too sensitive to reveal."[31] Outrage over the publication of the identities of American operatives in books and magazines prompted the passage of the Intelligence Identities Protection Act of 1982.[32] In other words, concerns about publications with bad motives existed long before WikiLeaks came on the scene; these concerns do not depend on the medium of communication or whether "professional" journalists are the ones making the publication decisions.

Another common argument for distinguishing WikiLeaks from the traditional media is that WikiLeaks stole its information, or solicited or encouraged sources to leak sensitive information. In her speech on Internet freedom, Secretary of State Clinton maintained that "the WikiLeaks incident began with a theft, just as if it had been executed by smuggling papers in a briefcase."[33] The problem is that there is no evidence that WikiLeaks stole any documents. Vice President Joseph Biden similarly argued that there was a difference between WikiLeaks' solicitation of classified information and the manner in which the traditional press acquires its information.[34] This distinction does not hold up, especially given the absence of any public evidence that WikiLeaks or Julian Assange actively solicited classified information. Indeed, it appears that *The New York Times*, taking a page from WikiLeaks' playbook, is considering

29. Cryptome was a predecessor to WikiLeaks. *See* Andrew Orlowski, *WikiLeaks Are For-Hire Mercenaries – Cryptome*, REGISTER, Dec. 7, 2010, http://www.theregister.co.uk/2010/12/07/cryptome_on_wikileaks/. GreenLeaks.com, GreenLeaks.org, and OpenLeaks.org are considered by some to be successors to WikiLeaks. *See* Mark Hosenball, *Exclusive: The Next Generation of WikiLeaks*, REUTERS, Jan. 28, 2011, http://www.reuters.com/article/2011/01/28/us-wikileaks-idUSTRE70R5A120110128.

30. *See* Edgar & Schmidt, *supra* note 19, at 965-966.

31. *Id*. at 1077.

32. 50 U.S.C. §§421-426 (2006).

33. Clinton, *supra* note 1.

34. Interview by David Gregory, host of Meet the Press, with Vice President Joseph Biden, NBC NEWS (Dec. 19, 2010), *available at* http://www.msnbc.msn.com/id/40720643/ns/meet_the_press-transcripts/ns/meet_the_press-transcripts.

establishing a virtual "drop box" where members of the public could deposit documents anonymously.[35] Several other organizations have already established portals for leaked information, including *The Wall Street Journal*[36] and *Al Jazeera*.[37]

The publication of national security secrets in a newspaper, magazine, or website may be as damaging to our national security interests as the transfer of secrets in the traditional espionage setting.[38] We must assume that our enemies consume our public media just as we do theirs; given this, publication of a national security secret in a newspaper might cause even more harm because the whole world potentially can learn about it. Nevertheless, Congress has traditionally been concerned with the dilemma of protecting legitimate national security secrets without undermining the sort of public debate that is essential in a democracy. Thus, when it was debating legislation that would become the Espionage Act of 1917, Congress rejected President Wilson's proposal for broad authority to punish the publication of national defense information.[39] The legislative history of the Espionage Act of 1917 "is replete with concern that these criminal statutes make use of appropriate standards of culpability to distinguish the morally innocent from the guilty."[40]

Congress has repeatedly recognized the importance of protecting legitimate criticism and examination of government actions every time it has amended the Espionage Act and related statutes.[41] Although recognizing the need to protect national security secrets, Congress has been concerned about passing laws that would unduly restrict the media's well-intentioned disclosures.[42] Thus, for example, in the debates surrounding the passage of the Intelligence Identities Protection Act of 1982, Congress repeatedly expressed concerns that any prohibitions on the disclosure of the identities of American agents should not cover academic studies of government programs and policies, or news media reporting of intelligence failures.[43] Recognizing that even the disclosure of an agent's identity could

35. Michael Calderone, *NY Times Considers Creating an "EZ Pass Lane for Leakers,"* YAHOO! NEWS, Jan. 25, 2011, http://news.yahoo.com/s/yblog_thecutline/20110125/ts_yblog_thecutline/ny-times-considers-creating-an-ez-pass-lane-for-leakers.

36. *See* SafeHouse, https://www.wsjsafehouse.com/.

37. *See About the Transparency Unit*, http://transparency. aljazeera.net/.

38. Edgar & Schmidt, *supra* note 19, at 934.

39. *Id*. at 940-941.

40. *Id*. at 1039.

41. *Id*. at 937 (noting that the Act's "legislative debates, amendments and conferences . . . may fairly be read as excluding criminal sanctions for well-meaning publication of information no matter what damage to the national security might ensue and regardless of whether the publisher knew its publication would be damaging").

42. *Id*. at 939.

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

be valuable, Congress provided that such disclosures are not actionable unless made with "reason to believe" that the disclosure would harm the United States, and that the disclosures were part of a "pattern or practice" of disclosure.[44]

Although Congress has historically appeared interested in protecting the freedom of the press and limiting executive power to control the debate on national security and military affairs, the plain language of the Espionage Act points a "loaded gun" at those who report on such topics.[45] For example, Section 793(e) prohibits the dissemination or retention of national security information by those in "unauthorized possession" of it, and the only applicable *mens rea* requirement in cases involving tangible materials is that the dissemination or retention be "willful."[46] With respect to the dissemination or retention of nontangible "information pertaining to the national defense," the government must prove that the offender has "reason to believe [the information] could be used to the injury of the United States or advantage a foreign nation."[47] Exactly what this provision requires is unclear. Some lower courts have held that the government must show that the offender had a "bad faith purpose either to harm the United States or aid a foreign government,"[48] but this construction is difficult to derive from the actual statutory language and arises from concerns that the phrase "national security information" would be unconstitutionally vague without it.

III. SUGGESTIONS FOR REFORM

Given that national security leaks play an important role in our democracy, Congress is faced with the difficult task of deciding under what circumstances the disclosure of national security information should be protected. The foregoing section illustrated the difficulties of line-drawing based on the medium of communication, the journalistic background of the publisher, or complicity in the leak itself. Instead of drawing lines on any of these bases, Congress should consider authorizing criminal sanctions against nongovernmental actors only in cases where the disclosure is made with an intent to harm the United States or with reckless indifference to any harm the disclosure would have.

At the outset, Congress must make a clear distinction between government employees (and contractors) and those who do not have a position of trust and confidentiality with the government. Very different

44. *Id*. at 51-52.
45. Edgar & Schmidt, *supra* note 19, at 936.
46. 18 U.S.C. §793(e) (2006).
47. *Id*.
48. *See*, *e.g*., United States v. Rosen, 445 F. Supp. 2d 602, 626 (E.D. Va. 2006).

policy considerations – as well as weaker First Amendment protections – apply in cases where individuals have obtained national security information as a result of a trusted relationship. It may well be that even in such cases there should be protection for the disclosure of information that has been improperly classified, or for the exposure of illegal or fraudulent activity.[49] In addition, it is appropriate to distinguish between the traditional espionage setting, where a government employee exposes secrets to a foreign power, and other circumstances in which the employee acts with the purpose of revealing information to the general public.[50]

Very different considerations come into play when deciding whether to criminalize the disclosure of national security information by third parties who did not obtain national security information as a result of a trusted relationship with the government. Although the legal landscape is unclear, the First Amendment arguably provides protection for the dissemination of any information that does not threaten grave, direct, and unavoidable harm to the United States.[51]

First, Congress should consider amending the Espionage Act to make clear what kind of information is covered by its provisions. Currently some of the Act's provisions apply to "information relating to the national defense." This category is vague and encompasses a potentially limitless universe of information. Instead, with respect to third parties who obtain unauthorized access to information, Congress should be specific about what information is subject to criminal sanctions. This has been the approach Congress has taken in more recent legislation, such as the Intelligence Identities Protection Act of 1982, which prohibits the identification of covert agents.[52]

Second, once Congress has identified specific topics that are especially sensitive, it should include rigorous culpability requirements. Determining the requisite level of intent is essential in drafting any criminal statute. In the criminal law context, the very same conduct may face dramatically different sanctions depending upon the intent of the actor. The same is true in the context of prosecutions based on the dissemination of national security information. The Espionage Act and related statutes contain a hodge-podge of intent standards that are hard to understand and difficult to apply.

49. *See* Geoffrey R. Stone, *Government Secrecy v. Freedom of the Press*, 1 HARV. L. & POL. REV. 185, 196 (2007).

50. The leading case involving a government employee who disclosed classified information to the press is *United States v. Morison*, in which the court rejected the defendant's argument that the Espionage Act is limited to the classic spying scenario but noted that the Act does permit heavier penalties for traditional espionage. *See* 844 F.2d 1057, 1065 (4th Cir. 1988).

51. *See* Stone, *supra* note 49, at 202.

52. 50 U.S.C. §§421-426 (2006).

The dissemination of information by nongovernment actors should be punishable only if the offender acted with the intent to harm the United States or with reckless indifference to such harm. This sort of intent standard would provide protection for all responsible publishers acting in good faith, no matter who they are or what medium they use for communication. Such a standard is similar to the "actual malice" standard the Supreme Court adopted in *New York Times Co. v. Sullivan*.[53] There, the Court held that given "a profound national commitment to the principle that debate on public issues should be uninhibited, robust, and wide-open,"[54] strict liability for the publication of false defamatory information about public officials would have a severe chilling effect on the press, which would be sure to make only statements that "steer far wider of the unlawful zone."[55] While recognizing that false defamatory speech can cause real harm to reputation, the Court determined that a public official can recover only if he demonstrates that the defendant published "with knowledge that [the speech] was false or with reckless disregard of whether it was false or not."[56] Just as the damage to our national security interests is the same regardless of the intent of the disseminator, the damage to a public official's reputation occurs regardless of the motivation of a defendant in a defamation action. Nevertheless, an intent requirement in both circumstances serves as an important way of promoting vigorous public debate while preserving the government's ability to act in the most egregious situations.

To be clear, this intent requirement does not turn on the motivation for disclosure. Even the most esteemed newspapers are driven in part by profit-seeking motives to increase circulation, just as some government employees engaged in traditional espionage do it for the money, not to harm the United States. Of course these sorts of pecuniary motivations might make it more difficult for a defendant to demonstrate that he was not recklessly indifferent to the harm the disclosure might cause, but they do not by themselves constitute intent to harm the United States or to aid our enemies.

Furthermore, the inclusion of a robust scienter requirement should not replace other important necessary elements. Proof of imminent and serious harm to U.S. interests must be demonstrated in addition to subjective intent to harm the United States. As Geoffrey Stone has persuasively argued, it would be inconsistent with the First Amendment to permit nongovernmental actors to be punished for the dissemination of national

53. 376 U.S. 254 (1964).
54. *Id*. at 270.
55. *Id*. at 279.
56. *Id*. at 279-280.

security information that does not in fact threaten imminent and serious harm.[57]

CONCLUSION

When considering whether and how to amend the Espionage Act and related statutes, Congress must keep in mind the important role that the press has played in our democracy throughout its history. In order to protect this vital function, it will be necessary at times to permit the publication of sensitive national security information that causes real harm. What is not necessary, however, is to protect the publication of such information if it is done with the intent to harm the United States – or aid its enemies – or with reckless disregard to any harm the publication will cause. To be sure, an intent requirement will not give the government the sort of control it might like over the information that is disseminated in the media, professional or otherwise. It is true that a stringent intent requirement would permit the press to publish information that might be useful to our enemies. But, as Congress has noted in its prior debates, this is the price we must pay in order to protect free debate. This approach places the burden squarely on the government to work harder to prevent and isolate leaks of national security information for which secrecy is essential.

57. *See* Stone, *supra* note 3, at 114-115.