4-2-2012

WikiLeaks and the Institutional Framework for National Security Disclosures

Patricia L. Bellia
Notre Dame Law School, patricia.l.bellia.2@nd.edu

THE YALE LAW JOURNAL

PATRICIA L. BELLIA

WikiLeaks and the Institutional Framework for National Security Disclosures

ABSTRACT. WikiLeaks' successive disclosures of classified U.S. documents throughout 2010 and 2011 invite comparison to publishers' decisions forty years ago to release portions of the Pentagon Papers, the classified analytic history of U.S. policy in Vietnam. The analogy is a powerful weapon for WikiLeaks' defenders. The Supreme Court's decision in the *Pentagon Papers* case signaled that the task of weighing whether to publicly disclose leaked national security information would fall to publishers, not the executive or the courts, at least in the absence of an exceedingly grave threat of harm.

The lessons of the *Pentagon Papers* case for WikiLeaks, however, are more complicated than they may first appear. The Court's per curiam opinion masks areas of substantial disagreement as well as a number of shared assumptions among the Court's members. Specifically, the *Pentagon Papers* case reflects an institutional framework for downstream disclosure of leaked national security information, under which publishers within the reach of U.S. law would weigh the potential harms and benefits of disclosure against the backdrop of potential criminal penalties and recognized journalistic norms. The WikiLeaks disclosures show the instability of this framework by revealing new challenges for controlling the downstream disclosure of leaked information and the corresponding likelihood of "unintermediated" disclosure by an insider; the risks of non-media intermediaries attempting to curtail such disclosures, in response to government pressure or otherwise; and the pressing need to prevent and respond to leaks at the source.

AUTHOR. Professor of Law and Notre Dame Presidential Fellow, Notre Dame Law School. I thank A.J. Bellia, Rick Garnett, Nicole Garnett, Andrea Matwyshyn, John Nagle, and Mary-Rose Papandrea for thoughtful discussions and comments, and research librarian Christopher O'Byrne for expert research assistance.

FEATURE CONTENTS

INTRODUCTION

For many observers, WikiLeaks' successive disclosures of classified U.S. documents throughout 2010 and 2011 invite comparison to publishers' decisions forty years ago to release portions of the Pentagon Papers, the classified analytic history of U.S. policy in Vietnam. The clash between the publishers and the government produced the celebrated decision of *New York Times Co. v. United States*, in which the Supreme Court held that the government had not carried the "heavy burden" of justifying a prior restraint against publication.[1] Although several Justices discussed the possibility that the newspapers could face criminal prosecution after the fact if they published material harmful to U.S. national security interests,[2] history has largely vindicated the newspapers' actions, as well as those of Daniel Ellsberg, the former government employee and RAND Corporation analyst who leaked the materials.[3]

The prominence of *New York Times Co. v. United States* in the First Amendment canon makes the Pentagon Papers analogy a powerful weapon for defenders of WikiLeaks and its key proprietor, Julian Assange. Ellsberg himself has characterized Assange as a "hero"[4] and has cited the "very strong" parallels between the WikiLeaks disclosures and the release of the Pentagon Papers.[5] A member of the legal team working with Assange has called the WikiLeaks disclosures "the Pentagon Papers case for the 21st Century."[6] For

1. 403 U.S. 713, 714 (1971) (quoting Org. for a Better Austin v. Keefe, 402 U.S. 415, 419 (1971)).

2. *See infra* text accompanying notes 98-103.

3. For a careful discussion of whether the disclosures harmed national security interests, see DAVID RUDENSTINE, THE DAY THE PRESSES STOPPED: A HISTORY OF THE PENTAGON PAPERS CASE 328-29 (1996). Professor Rudenstine concludes that although the materials the newspapers disclosed did not seriously harm national security, the leaked study later dubbed the Pentagon Papers did in fact contain material that could have seriously harmed national security interests if it had been disclosed. *Id.* at 329. For a critique of that perspective, see INSIDE THE PENTAGON PAPERS 147-53 (John Prados & Margaret Pratt Porter eds., 2004).

4. Anna Mulrine, *Pentagon Papers vs. WikiLeaks: Is Bradley Manning the New Ellsberg?*, CHRISTIAN SCI. MONITOR, June 13, 2011, http://www.csmonitor.com/USA/Military/2011/0613/Pentagon-Papers-vs.-WikiLeaks-Is-Bradley-Manning-the-new-Ellsberg (quoting Daniel Ellsberg).

5. Paul Farhi & Ellen Nakashima, *Is WikiLeaks the Pentagon Papers, Part 2? Parallels, and Differences, Exist*, WASH. POST, July 27, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/07/26/AR2010072605410.html (quoting Daniel Ellsberg).

6. Charles Homans, *Alan Dershowitz Joins Assange Legal Team: WikiLeaks Is "21st Century Pentagon Papers,"* FOREIGN POL'Y (Feb. 15, 2011, 3:56 PM), http://wikileaks.foreignpolicy.com/

commentators who question WikiLeaks' actions, in contrast, the differences between the disclosures overwhelm any similarities.[7] The Pentagon Papers analyzed decisionmaking at the highest levels of the government over more than two decades and, in the view of many observers, confirmed that successive administrations had misled the American public about the objectives and conduct of the Vietnam conflict.[8] The leaked documents on the Afghan and Iraq conflicts, by contrast, are a collection of unedited raw materials, including first-hand incident and intelligence reports from military personnel on the ground.[9] The diplomatic cables released between November 2010 and September 2011 include sensitive communications of far-flung embassies dealing with a range of topics, from strategic concerns in the Middle East,[10] to corruption in foreign governments,[11] to assessments of foreign leaders'

posts/2011/02/15/alan_dershowitz_joins_assange_legal_team_wikileaks_is_21st_century_pentagon_papers (quoting Professor Alan Dershowitz).

7. *See, e.g.*, Derek E. Bambauer, *Consider the Censor*, 1 WAKE FOREST J.L. & POL'Y 31 (2011); *see also The Leonard Lopate Show: Neil Sheehan on Leaks and Wikileaks*, 1:17-2:04 (WNYC radio broadcast July 29, 2010), http://www.wnyc.org/shows/lopate/2010/jul/29/neil-sheehan-leaks-and-wikileaks (featuring an interview with a recipient of the Pentagon Papers who argues that the WikiLeaks disclosures, while valuable, are vastly different from the Pentagon Papers).

8. *See, e.g.*, RUDENSTINE, *supra* note 3, at 332 (noting that the dominant theme in the aftermath of the disclosures was "whether the documents proved that prior administrations, especially the Johnson administration, had deceived the public about America's entanglement in Vietnam").

9. *See* Nick Davies & David Leigh, *Afghanistan War Logs: Massive Leak of Secret Files Exposes Truth of Occupation*, GUARDIAN, July 25, 2010, http://www.guardian.co.uk/world/2010/jul/25/afghanistan-war-logs-military-leaks; David Leigh, *Iraq War Logs: An Introduction*, GUARDIAN, Oct. 22, 2010, http://www.guardian.co.uk/world/2010/oct/22/iraq-war-logs-introduction. For selections of the documents, see, for example, *Afghanistan: The War Logs*, GUARDIAN, http://www.guardian.co.uk/world/the-war-logs+content/table (last visited Oct. 20, 2011); *Secret Dispatches from the War in Iraq*, N.Y. TIMES, http://www.nytimes.com/interactive/world/iraq-war-logs.html (last visited Oct. 20, 2011); and *Text from a Selection of the Secret Dispatches*, N.Y. TIMES, http://www.nytimes.com/interactive/world/26warlogs.html (last visited Oct. 20, 2011).

10. *See, e.g.*, David E. Sanger, James Glanz & Jo Becker, *Around the World, Distress Over Iran*, N.Y. TIMES, Nov. 28, 2010, http://www.nytimes.com/2010/11/29/world/middleeast/29iran.html.

11. *See, e.g.*, Rob Evans, Luke Harding & John Cooper, *WikiLeaks Cables: Berlusconi "Profited from Secret Deals" with Putin*, GUARDIAN, Dec. 2, 2010, http://www.guardian.co.uk/world/2010/dec/02/wikileaks-cables-berlusconi-putin; Luke Harding, *WikiLeaks Cables Condemn Russia as 'Mafia State,'* GUARDIAN, Dec. 1, 2010, http://www.guardian.co.uk/world/2010/dec/01/wikileaks-cables-russia-mafia-kleptocracy; Scott Shane, Mark Mazzetti & Dexter Filkins, *Cables Depict Afghan Graft, Starting at Top*, N.Y. TIMES, Dec. 2, 2010, http://www.nytimes.com/2010/12/03/world/asia/03wikileaks-corruption.html.

personalities and habits.[12] The Pentagon Papers episode, moreover, involved established publishers who claimed to be sensitive to the need to balance the public's right to know against U.S. national security concerns.[13] Even to those within the established news organizations that initially partnered with WikiLeaks to analyze and disseminate classified information in 2010, WikiLeaks' and Assange's motives are far less clear.[14]

Despite the obvious differences between the *Pentagon Papers* case and the WikiLeaks saga, both controversies presented the same fundamental institutional question: *Who decides* when the need for public access to certain leaked national security information outweighs the potential harm that dissemination might cause? In holding in *New York Times Co. v. United States* that the government had not overcome the presumption against prior restraints, the Supreme Court answered that, as to the Pentagon Papers, the decision fell to the *Times*, the *Washington Post*, and the other news outlets that held copies of the documents. The question is what insight that case offers for the emergence and evolution of WikiLeaks forty years later.

The Court's seemingly straightforward approach to the institutional question in *New York Times Co. v. United States* masks a number of complexities. First, as a doctrinal matter, the Court's brief per curiam opinion left open whether a different balance of public interest and harm could ever justify a prior restraint on publication—a question that a majority of Justices,

12. *See, e.g.*, Rory Carroll, *Hillary Clinton Questions Cristina Kirchner's Mental Health*, GUARDIAN, Nov. 29, 2010, http://www.guardian.co.uk/world/2010/nov/29/hillary-clinton-cristina-kirchner-stress; David Leigh, *WikiLeaks Cables: Muammar Gaddafi and the 'Voluptuous Blonde,'* GUARDIAN, Dec. 7, 2010, http://www.guardian.co.uk/world/2010/dec/07/wikileaks-cables-gaddafi-voluptuous-blonde.

13. *See* Bambauer, *supra* note 7, at 34 ("As the paper of record in the United States, the *Times* followed carefully a set of ethical precepts derived both from journalistic norms and from underlying American values.").

14. *See, e.g.*, John F. Burns & Ravi Somaiya, *Who Is Julian Assange?*, *in* OPEN SECRETS: WIKILEAKS, WAR, AND AMERICAN DIPLOMACY 25, 33 (Alexander Star ed., 2011) (noting the tension between WikiLeaks' stated mission of impartiality and what Assange described as a fight against global injustice, "the judgment of which, it seemed clear, would be rendered primarily by himself"); John F. Burns & Ravi Somaiya, *WikiLeaks Founder on the Run, Trailed by Notoriety*, N.Y. TIMES, Oct. 23, 2010, http://www.nytimes.com/2010/10/24/world/24assange.html (claiming that some of Assange's associates abandoned him because of his "erratic and imperious behavior, and a nearly delusional grandeur unmatched by an awareness that the digital secrets he reveals can have a price in flesh and blood"). For claims that these accounts reflect the mainstream media's attempt to marginalize Assange, see Yochai Benkler, *A Free Irresponsible Press: Wikileaks and the Battle over the Soul of the Networked Fourth Estate*, 46 HARV. C.R.-C.L. L. REV. 311, 325-26, 386-94 (2011); and Glenn Greenwald, *The Nixonian Henchmen of Today: At the NYT*, SALON (Oct. 24, 2010, 11:25 AM), http://www.salon.com/2010/10/24/assange_2.

in separate opinions, answered in the affirmative. In other words, a majority of Justices accepted that in certain factual contexts, a court's assessment of the balance of public interest and harm—informed, presumably, by the executive's assessment—could displace a publisher's.[15] Second, the Court's conclusion that, except in rare cases, the executive could not invoke the power of the judiciary to control the release of documents leaked to the press was not an endorsement of a *source*'s power to assess the balance of public interest and harm. The separate opinions in the case illustrate key assumptions shared by a number of the Justices: that the possibility of criminal liability, and an ethical responsibility to prevent harm, would shape how the publishers used the Pentagon Papers.[16] Put another way, *New York Times Co. v. United States* does not presume a shared conception of the public interest and harm among the source and the potential publisher. In fact, it presumes the publisher's intermediation, even with respect to information that the publisher cannot be enjoined from disclosing. Finally, although *New York Times Co. v. United States* essentially recognized a First Amendment privilege for publishers to assess the threats and benefits of disclosure (at least up to the point at which a court could enjoin disclosure), the case acknowledged no parallel privilege for the *source* to release information up to that point. That is, the *Pentagon Papers* case presumed, or at least tolerated, an asymmetry: the government could withhold—and perhaps punish a source for releasing—information that it could not enjoin a publisher from further disclosing.

The WikiLeaks disclosures test a number of premises underlying the *Pentagon Papers* case. The disclosures first call into question the premise that a U.S. court could effectively restrain publication of national security information, even information presenting an exceedingly grave risk of harm. Second, certain aspects of the WikiLeaks disclosures threaten the model of established publishers assessing the balance of harm and the public interest against the backdrop of potential criminal penalties or recognized journalistic norms. The Justices who preliminarily considered a publisher's liability for secondary transmission of leaked information may have misjudged the risks of criminal liability. Third, WikiLeaks' global operating platform—which allows the organization to broker information-sharing deals with multiple publishers in a fragmented and global media marketplace—raises questions about whether public disclosures of national security information will in fact hew to a set of recognized journalistic norms.

15. *See infra* notes 46-57 and accompanying text.

16. *See infra* notes 98-108 and accompanying text.

The WikiLeaks disclosures, in short, reveal that some of the presumed constraints on downstream publication of leaked national security information may be illusory. Far from mapping neatly onto the *Pentagon Papers* case, the WikiLeaks disclosures require that we rethink the institutional framework the *Pentagon Papers* case presumes for controlling the secondary transmission of leaked national security information. The WikiLeaks disclosures demonstrate the challenge of controlling the secondary transmission of leaked information and the corresponding likelihood of "unintermediated" disclosure by an insider; the risks of non-media intermediaries attempting to curtail such disclosures, as a response to government pressure or otherwise; and the pressing need to prevent and respond to leaks at the source.

The Essay proceeds as follows. Part I explores *New York Times Co. v. United States*, charting its doctrinal limits and the Justices' shared assumptions, with particular focus on the underlying institutional questions. Part II assesses the actions of WikiLeaks and its media partners in light of the premises of the *Pentagon Papers* case. The WikiLeaks disclosures call into question two key premises behind the opinions in the case: that the secondary transmission of leaked national security information will involve a publisher within the reach of U.S. law, and that transmission will be shaped by the risk of criminal liability. A third premise, that publishers will self-censor to avoid disclosing harmful national security information, is difficult to evaluate in the context of the WikiLeaks disclosures, but the global and fragmented media marketplace suggests that self-censorship is less likely to occur. Part III offers some preliminary thoughts on how we should approach the problem of leaks in light of the shift away from the institutional framework assumed in the *Pentagon Papers* case. After discussing the government's narrow options for limiting the secondary transmission of leaked information and the promise and risks of relying on other non-media intermediaries to do so, I turn to what should be a major focus of reform efforts in this area: shaping the legal and technological environment for leaks.

I. RECOVERING THE PENTAGON PAPERS CASE

In 1967, Secretary of Defense Robert McNamara, increasingly disaffected with U.S. involvement in the conflict in Vietnam, commissioned a secret study on U.S. decisionmaking in Southeast Asia. The classified study, completed in January 1969, comprised 47 volumes and included some 3000 pages of analysis

accompanied by 4000 pages of primary documents.[17] In its June 13, 1971, edition, the *New York Times* devoted more than six pages to what would come to be known as the "Pentagon Papers." A front-page story described the "massive study" as a "great archive of government decision-making on Indochina over three decades."[18] The study's authors, the *New York Times* reported, had concluded that the predominant American interest in Vietnam transformed over time, from an interest in containment of communism to a defense of American influence and prestige, "in both stages irrespective of conditions in Vietnam."[19] In connection with its story, the *New York Times* excerpted several cables, position papers, and memoranda exchanged among high-level administration officials, including McNamara, President Lyndon Johnson, and the Chairman of the Joint Chiefs of Staff.[20]

The *New York Times*'s decision to publish the classified excerpts and the Nixon Administration's response the following evening launched sixteen days of frenetic court proceedings, culminating on June 30 in the Supreme Court's decision. Others have analyzed these events in detail,[21] and I need not duplicate their work. My goal, rather, is to sketch the institutional structure the Supreme Court envisioned for the disclosure of leaked national security information. Section I.A describes the proceedings and identifies the key legal and factual questions the case presented. Section I.B explores the Court's brief per curiam opinion and the six concurring and three dissenting opinions that shed light on the decision. The Court's holding that the government had not justified a prior restraint left in the hands of the publishers the task of weighing the public interest in disclosure against the projected harm. A number of Justices, however, assumed that the possibility of criminal liability and responsible journalism would shape the publishers' decisions. Section I.C sets the stage for

17. Neil Sheehan, *Introduction* to NEIL SHEEHAN ET AL., THE PENTAGON PAPERS AS PUBLISHED BY THE NEW YORK TIMES, at ix, ix (Bantam Books 1971) [hereinafter PENTAGON PAPERS]; *see* INSIDE THE PENTAGON PAPERS, *supra* note 3, at 17 (noting the January 1969 completion date).

18. Neil Sheehan, *Vietnam Archive: Pentagon Study Traces 3 Decades of Growing U.S. Involvement*, N.Y. TIMES, June 13, 1971, http://www.nytimes.com/books/97/04/13/reviews/papers-overview.html. In addition to the front page stories, the *Times*'s coverage extended from pages 35-40 of the June 13 edition.

19. *Id.*

20. *See, e.g.*, *'64 Memo by Joint Chiefs of Staff Discussing Widening of the War*, N.Y. TIMES, June 13, 1971, at 35; *McNamara Report to Johnson on the Situation in Saigon in '63*, N.Y. TIMES, June 13, 1971, at 35.

21. *See, e.g.*, RUDENSTINE, *supra* note 3; SANFORD J. UNGAR, THE PAPERS & THE PAPERS: AN ACCOUNT OF THE LEGAL AND POLITICAL BATTLE OVER THE PENTAGON PAPERS (Notable Trials Library 1996) (1972).

examining the WikiLeaks disclosures through the lens of the *Pentagon Papers* case.

A. The Court Proceedings

After the *Times* published the second installment of its series on the Pentagon Papers, Attorney General John Mitchell sent a telegram to the *Times* demanding that it cease publication and return the materials to the U.S. government.[22] The telegram claimed that the Espionage Act of 1917, as amended, prohibited publication of the material and that publication would cause "irreparable injury" to the United States.[23] The following day, as the *Times* published the third installment, the Department of Justice filed suit in federal district court in New York and moved for a temporary restraining order and a preliminary injunction against continued publication.[24] The district judge assigned to the case—Judge Murray Gurfein, sworn in as a district court judge less than a week before[25]—granted a temporary restraining order barring the *Times* from "publishing or further disseminating or disclosing" the classified materials.[26] The *Times*'s then-undisclosed source was Daniel Ellsberg, a RAND Corporation analyst who had worked on a portion of the study.[27]

After the court issued a temporary restraining order against the *Times*, Ellsberg provided portions of the study to the *Washington Post*, which began publishing its own series on the documents on June 18.[28] That afternoon, the Department of Justice sought a temporary restraining order and preliminary injunction against the *Washington Post* in federal district court in Washington, D.C., where the case came before Judge Gerhard A. Gesell. After Judge Gesell refused to issue the temporary restraining order, a panel of the D.C. Circuit

22. *See* UNGAR, *supra* note 21, at 120.

23. *Id.*

24. *See id.* at 124-25.

25. *See* James L. Oakes, *Judge Gurfein and the Pentagon Papers*, 2 CARDOZO L. REV. 5, 5 (1980).

26. *See* United States v. N.Y. Times Co., 328 F. Supp. 324, 325 (S.D.N.Y.), *rev'd*, 444 F.2d 544 (2d Cir.) (in banc), *rev'd*, 403 U.S. 713 (1971) (per curiam).

27. *See* DANIEL ELLSBERG, SECRETS: A MEMOIR OF VIETNAM AND THE PENTAGON PAPERS 186 (2002); PETER SCHRAG, TEST OF LOYALTY: DANIEL ELLSBERG AND THE RITUALS OF SECRET GOVERNMENT 35-38 (1974); UNGAR, *supra* note 21, at 29.

28. *See* UNGAR, *supra* note 21, at 135, 147, 149. Ellsberg claimed that he ultimately provided the study to seventeen other newspapers in an effort to evade the restraints on publication imposed by the courts. ELLSBERG, *supra* note 27, at xii.

reversed, although the reversal came too late to prevent publication of the *Post*'s second installment.[29]

With each paper temporarily barred from continuing their series on the documents, the two district courts held hearings on the government's requests for preliminary injunctive relief. Recognizing that proof of the government's claims of irreparable injury would depend on the contents of the underlying classified materials, each judge scheduled both a public hearing and an in-camera session, thus inviting the government to identify, in a confidential setting, any portion of the forty-seven volumes that, if released, could damage national security. Neither court was convinced, and each district court denied the government's request for preliminary injunctive relief, Judge Gurfein on June 19[30] and Judge Gesell on June 21.[31] The government appealed both cases, and the courts of appeals reached opposite results. The Second Circuit remanded the case for further proceedings,[32] whereas the D.C. Circuit affirmed the district court's denial of the preliminary injunction.[33] By June 25, with stays in place that continued to bar the *Times* and the *Post* from publishing any further installments, both cases were ripe for the Supreme Court's consideration. The Court granted writs of certiorari and scheduled an unusual Saturday oral argument session for the following day.[34]

On June 30, four days after oral argument, the Supreme Court, by a vote of 6-3, issued an unsigned opinion affirming the judgment of the D.C. Circuit, reversing the order of the Second Circuit, and vacating the stays that prevented publication. The Court's brief per curiam opinion stated only that the government bears a heavy burden in justifying a prior restraint, and that the Court agreed with both district courts that the government had not met that burden.[35] The six-Justice consensus on this narrow holding, however, masked

29. *See* UNGAR, *supra* note 21, at 159-60.

30. *N.Y. Times Co.*, 328 F. Supp. at 331.

31. United States v. Wash. Post Co., No. 71 Civ. 1235 (D.D.C. June 21, 1971), *excerpts reprinted in* THE PENTAGON PAPERS AND THE COURTS: A STUDY IN FOREIGN POLICY-MAKING AND FREEDOM OF THE PRESS 98 (Martin Shapiro ed., 1972) [hereinafter THE PENTAGON PAPERS AND THE COURTS].

32. The Second Circuit heard the case in banc, without a prior panel hearing, and voted 5-3 to remand. United States v. N.Y. Times Co., 444 F.2d 544 (2d Cir.) (in banc), *rev'd*, 403 U.S. 713 (1971) (per curiam); *see infra* note 71 and accompanying text.

33. United States v. Wash. Post Co., 446 F.2d 1327, 1328 (D.C. Cir.) (en banc) (per curiam), *aff'd sub nom.* United States v. N.Y. Times Co., 403 U.S. 713 (1971).

34. United States v. Wash. Post Co., 403 U.S. 943 (1971) (granting certiorari); *see* UNGAR, *supra* note 21, at 211-12.

35. *N.Y. Times Co.*, 403 U.S. at 714.

the complexities of other related questions, including whether a court could ever block publication of harmful national security information and, if so, on what showing of harm. Although the Court's opinion did not address these questions directly, all nine Justices filed separate opinions. Not only do these opinions refine our understanding of the Court's First Amendment holding and the questions it left unanswered; they also reveal the key assumptions operating behind the decision—assumptions that bear upon our understanding of the WikiLeaks disclosures.

B. The Decisions: Common Ground and Divisions

At its most basic level, the *Pentagon Papers* case presented an institutional question: *who decides* when the public interest in disclosure of leaked national security information outweighs the potential harm of disclosure? On the facts of the case before them, the Justices answered that the publishers must be left to decide. Throughout the litigation, however, the parties and the courts wrestled with three key issues: (1) whether a court could ever block publication of harmful national security information, or whether an injunction would always constitute an unlawful "prior restraint"; (2) if injunctive relief is sometimes permissible, what showing of harm is required; and (3) whether the government's evidence met that threshold. These questions have continuing doctrinal relevance, including with respect to the WikiLeaks disclosures. This Section considers the insights that the separate opinions offer on these questions as a means of understanding the Court's holding. Beyond charting the doctrinal limits of the *Pentagon Papers* case, the separate opinions, I argue, shed light on certain shared assumptions about the institutional framework for disclosure of leaked national security information.

1. The Legality of Prior Restraints

The crux of the government's claims against the newspapers was that continued publication of classified material from the Pentagon Papers study would cause irreparable injury to the United States. The district courts initially split on a threshold question: whether a court can ever block the press from publishing truthful information of public value. Judge Gurfein's decision to grant a temporary restraining order barring further publication[36] reflected a premise that a court could, in some circumstances, lawfully enjoin the

36. *See* United States v. N.Y. Times Co., 328 F. Supp. 324, 325 (S.D.N.Y.), *rev'd*, 444 F.2d 544 (2d Cir.) (in banc), *rev'd*, 403 U.S. 713 (1971) (per curiam).

publication of information claimed to threaten national security. In the *Post* case, by contrast, Judge Gesell rejected that premise, on the ground that criminal sanctions are the government's sole remedy for publication of such information.[37] The U.S. Court of Appeals for the D.C. Circuit reversed this ruling and remanded the case to the district court for a hearing.[38]

In considering whether the executive could lawfully invoke the power of a court to block publication, each of the district courts, as well as the D.C. Circuit, relied in part on the Supreme Court's decision in *Near v. Minnesota*.[39] In *Near*, the Supreme Court had invalidated as an unlawful prior restraint an injunction prohibiting publication of a newspaper alleged to be "malicious, scandalous and defamatory" under Minnesota's public nuisance law.[40] In dicta, however, the Court wrote that the protection against prior restraints "is not absolutely unlimited."[41] Quoting *Schenck v. United States*, the Court observed in *Near* 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."[42] The Court offered examples of speech that would be unprotected, including "publication of the sailing dates of transports or the number and location of troops."[43]

Despite the D.C. District Court's initial holding that ex post criminal punishment is the sole remedy for disclosure of information that is potentially harmful to national security, neither the *Times* nor the *Post* continued to press the argument that the First Amendment forbids all prior restraints.[44] Rather, they conceded that a court could enjoin publication of harmful national security information in exceedingly narrow circumstances[45]—circumstances, they claimed, not presented in this case.

37. *See Wash. Post Co.*, 446 F.2d at 1323 (noting the district court's initial ruling); *see also* United States v. Wash. Post Co., No. 71 Civ. 1235 (D.D.C. June 18, 1971), *excerpts reprinted in* THE PENTAGON PAPERS AND THE COURTS, *supra* note 31, at 98.

38. *Wash. Post Co.*, 446 F.2d at 1323.

39. Near v. Minnesota *ex rel.* Olson, 283 U.S. 697 (1931).

40. *Id.* at 702.

41. *Id.* at 716.

42. *Id.* (quoting Schenck v. United States, 249 U.S. 47, 52 (1919)).

43. *Id.*

44. *See* RUDENSTINE, *supra* note 3, at 104, 201, 285.

45. *See* Post*'s Brief Against Barring Series: Memo Cites Government's Burden in a First Amendment Case*, WASH. POST, June 22, 1971, at A10. The *Times* argued that the government lacked any basis for seeking injunctive relief, but it did not argue that the First Amendment prohibited all prior restraints. *See* Memorandum of Defendant N.Y. Times Co. in Opposition to

In holding that the government had not met the "heavy burden" of justifying a prior restraint, the Court sidestepped the threshold question of whether the government could ever seek to enjoin publication based on projected harm to national security. Although the case no longer squarely presented this question, in their concurring opinions Justices Black and Douglas took the view that a prior restraint is never legitimate. Justice Black, joined by Justice Douglas, maintained his absolutist view of the First Amendment: "Both the history and language of the First Amendment support the view that the press must be left free to publish news, whatever the source, without censorship, injunctions, or prior restraints."[46] Justice Douglas, joined by Justice Black, likewise claimed that the First Amendment "leaves . . . no room for governmental restraint on the press."[47]

The remaining seven Justices, by contrast, acknowledged the possibility of an injunction against publication of material that could damage national security. The three dissenting Justices argued that the lower courts should consider the government's claims more fully—a position inconsistent with the view that a court can never block publication of material claimed to jeopardize national security interests.[48] Three concurring Justices—Justices Stewart, White, and Marshall—considered a mix of separation of powers and First Amendment concerns. Each Justice focused in part on the fact that Congress had not expressly authorized the President to seek injunctive relief, and indeed had rejected proposed legislation that would have given the President authority to do so.[49] Justice White (joined by Justice Stewart) and Justice Marshall, however, accepted the premise that *Congress* could authorize the President to seek injunctive relief in appropriately defined circumstances.[50] This position, too, was inconsistent with a view that the First Amendment categorically bars restraints on publication. Justice Marshall and Justice White even acknowledged the possibility that in some cases, the President may have inherent authority to invoke the equitable jurisdiction of the courts to prevent

Issuance of Preliminary Injunction at 13, United States v. N.Y. Times Co., 328 F. Supp. 324 (S.D.N.Y. 1971) (No. 71 Civ. 2662). Professor Rudenstine argues that the *Times*'s approach reflected the view of *Times* attorney Professor Alexander Bickel that the *Times* would have a better chance of prevailing in the Supreme Court if it conceded that the government could enjoin publication in limited circumstances. *See* RUDENSTINE, *supra* note 3, at 104.

46. N.Y. Times Co. v. United States, 403 U.S. 713, 717 (1971) (Black, J., concurring).

47. *Id.* at 720 (Douglas, J., concurring).

48. *Id.* at 752 (Burger, C.J., dissenting); *id.* at 758-59 (Harlan, J., dissenting); *id.* at 761-62 (Blackmun, J., dissenting).

49. *Id.* at 734 (White, J., concurring); *id.* at 746-47 (Marshall, J., concurring).

50. *Id.* at 731 (White, J., concurring); *id.* at 746-47 (Marshall, J., concurring).

publication of material dangerous to national security.[51] The burden that the government would have to meet, however, would be "very heavy" in the absence of statutory authority.[52]

Even Justice Brennan, whose opinion scholars sometimes align with Justice Black's and Justice Douglas's in terms of its absolutism,[53] recognized the possibility that the executive could seek to enjoin publication of damaging national security information. To be sure, Justice Brennan's position was not a great distance from Justice Black's or Justice Douglas's, for he condemned even the granting of temporary relief barring publication by the *Times* and the *Post*. Justice Brennan nevertheless acknowledged that "[o]ur cases . . . have indicated that there is a single, extremely narrow class of cases in which the First Amendment's ban on prior judicial restraint may be overridden."[54] For Justice Brennan, cases falling within that narrow class could include Chief Justice Hughes's examples in *Near*, involving wartime publication of "sailing dates of transports or the number and location of troops," as well as peacetime publication of information that "would set in motion a nuclear holocaust."[55] Justice Brennan concluded, however, that "in neither of these actions has the Government presented or even alleged that publication of items from or based upon the material at issue would cause the happening of an event of that nature."[56] Thus, Justice Brennan saw the First Amendment not as an absolute bar to judicial restraint of publication in any case, but as "an absolute bar to the imposition of judicial restraints *in circumstances of the kind presented by these cases*," where the government's claims were "predicated upon surmise or conjecture that untoward consequences may result."[57]

2. Required Showing of Harm

In light of the fact that seven Justices declined to exclude the possibility of injunctive relief to prevent publication of material damaging to national

51. *Id.* at 731 n.1 (White, J., concurring); *id.* at 742 (Marshall, J., concurring).

52. *Id.* at 731 (White, J., concurring).

53. *See, e.g.*, John Cary Sims, *Triangulating the Boundaries of the Pentagon Papers*, 2 WM. & MARY BILL RTS. J. 341, 349 n.23 (1993). Justice Black even exempted Justice Brennan's opinion from his criticism of other Justices' willingness to tolerate a prior restraint. *See N.Y. Times Co.*, 403 U.S. at 715 (Black, J., concurring).

54. *N.Y. Times Co.*, 403 U.S. at 726 (Brennan, J., concurring).

55. *Id.*

56. *Id.*

57. *Id.* at 725 (emphasis added).

security, the next logical question is what showing the government would have to make to secure such relief. Throughout the litigation, the parties disagreed about what showing would entitle the government to that relief and whether the government had met that burden. The examples the Court offered in *Near v. Minnesota* provided a starting point, but the lower courts wrestled with how to translate those examples—"publication of the sailing dates of transports or the number and location of troops"[58]—into a workable test. Judge Gurfein noted that the *Near* Court's examples "accent how limited is the field of security protection in the context of the compelling force of First Amendment right,"[59] and he concluded that the government had not demonstrated that the *New York Times* was "about to publish information or documents *absolutely vital to current national security*."[60] On appeal, the Second Circuit framed the question as whether certain materials would pose a "*grave and immediate danger to the security* of the United States."[61] The D.C. Circuit, meanwhile, synthesizing Judge Gesell's inquiry, asked whether publication of the material in question would "*gravely prejudice the defense interests* of the United States or *result in irreparable injury* to the United States."[62]

At oral argument in the Supreme Court, each of the parties to some degree embraced the legal standards proposed in the courts below. The Justices' questioning, however, revealed the difficulties of applying these standards. At least three issues emerged from the Justices' questioning: (1) What *scope* or *magnitude* must the predicted harmful event have to justify injunctive relief?[63]

58. Near v. Minnesota *ex rel.* Olson, 283 U.S. 697, 716 (1931).

59. United States v. N.Y. Times Co., 328 F. Supp. 324, 331 (S.D.N.Y.), *rev'd*, 444 F.2d 544 (2d Cir.) (in banc), *rev'd*, 403 U.S. 713 (1971) (per curiam).

60. *Id.* at 330 (emphasis added).

61. *N.Y. Times Co.*, 444 F.2d at 544 (emphasis added).

62. United States v. Wash. Post Co., 446 F.2d 1327, 1328 (D.C. Cir.) (en banc) (per curiam) (emphases added), *aff'd sub nom.* United States v. N.Y. Times Co., 403 U.S. 713 (1971).

63. On the question of the scope or magnitude of the predicted harm, Justice Stewart put the following hypothetical to Professor Alexander Bickel, attorney for the *Times*:

> Let us assume that when the members of the Court go back and open up this sealed record we find something there that absolutely convinces us that its disclosure would result in the sentencing to death of 100 young men whose only offense had been that they were 19 years old, and had low draft numbers. What should we do?

Professor Bickel conceded that if the causal link between publication and the feared result was direct and immediate, then publication could be enjoined—that the feared event need not "be of cosmic nature" for an injunction to issue. Transcript of Oral Argument, N.Y. Times Co. v. United States, 403 U.S. 713 (1971) (Nos. 1873 & 1885), *reprinted in* LANDMARK BRIEFS AND ARGUMENTS OF THE SUPREME COURT OF THE UNITED STATES: CONSTITUTIONAL LAW 213, 239-40 (Philip B. Kurland & Gerhard Casper eds., 1975).

(2) Must the test have a *temporal* component, as the Second Circuit's "grave *and immediate*" formulation suggests? (3) How tight must the *causal nexus* be between the information to be published and the predicted harm?

The Court's per curiam opinion offers no guidance on these questions, simply characterizing the government's burden as "heavy" and unmet. Nor is it possible to distill a common test from the various concurring and dissenting opinions. Part of the difficulty lies in the fact that the materials that the Justices found not to justify an injunction were under seal at the time of the case and could not be discussed in the public filings or opinions. Because the materials are now available, some general observations are possible.[64]

Throughout the course of the litigation, the government narrowed its claim about which materials within the Pentagon Papers study threatened to harm national security interests. The government's initial claim was that the courts should suppress publication of the entire Pentagon Papers study and that the study's "top secret" classification, without more concrete evidence of harm, justified that suppression. By the time the Supreme Court heard oral argument in the case, the government had identified specific materials that would cause harm if not suppressed, including material that, although relating to past events, was claimed to threaten current diplomatic relations and current military efforts. Ultimately, then, the case sheds some light on whether an impairment of diplomatic relations can ever sustain injunctive relief and on the strength of the causal nexus between the disclosure and the asserted harm, particularly when the materials in question relate to past events.

Although it was unclear precisely what materials the newspapers had received, each district court proceeded on the assumption that the newspapers possessed the entire forty-seven-volume McNamara study. The in camera hearings made it possible for the government to identify, in a confidential setting, any portion of the forty-seven volumes that, if released, would damage national security. In both district courts, however, the government took the position that the "top secret" classification of the Pentagon study was sufficient to establish that unauthorized disclosure of the study would irreparably damage national security interests.[65]

In the closed hearing in the *Times* case, government witnesses identified no specific documents supporting the claim that disclosure of the study would irreparably harm national security. The strategy proved disastrous. In holding that the government was not entitled to preliminary injunctive relief, Judge Gurfein acknowledged that he himself had not had the opportunity to review

64. For a detailed assessment of the material filed under seal, see Sims, *supra* note 53, at 375-96.

65. *See* RUDENSTINE, *supra* note 3, at 105, 204.

the forty-seven volumes. He observed, however, that he "did give the Government an opportunity to pinpoint what it believed to be vital breaches to our national security of sufficient impact to controvert the right of a free press."[66] The government's arguments, Judge Gurfein wrote, amounted to claims that, "by reference to the totality of the studies an enemy might learn something about United States methods which he does not know, that references to past relationships with foreign governments might affect the conduct of our relations in the future."[67] For Judge Gurfein, these generalized claims were not enough to justify a prior restraint.

In the *Post* case, the government likewise sought to avoid identifying specific portions of the study that would, if released, irreparably damage national security. The government claimed that all forty-seven volumes of the study should be suppressed, notwithstanding the fact that some portions of the study contained material already made public, including a volume that contained only public statements of prior administrations.[68] The government did offer some testimony in affidavit form identifying specific dangers the study presented.[69] Despite the greater specificity, however, the government's claims still fell short: Judge Gesell characterized the study as involving "material in the public domain and other material that was 'top secret' when written long ago but not clearly shown to be such at the present time."[70]

The district courts' reactions to the government's failure to pinpoint material that would irreparably harm U.S. national security interests prompted a dramatic shift in strategy. When the government renewed its request for a preliminary injunction before a panel of the Second Circuit, it submitted under seal a "Special Appendix" designating specific documents that, the government claimed, would damage national security if made public. Sitting in banc in the first instance, the Second Circuit voted 5-3 to remand the case to Judge Gurfein to review the Special Appendix, and any materials the government added to it by June 25, 1971, to determine whether any such items "pose such grave and immediate danger to the security of the United States as to warrant their

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

67. *Id.* at 327.

68. RUDENSTINE, *supra* note 3, at 205.

69. United States v. Wash. Post Co., 446 F.2d 1327, 1328 (D.C. Cir.) (en banc) (per curiam), *aff'd sub nom.* United States v. N.Y. Times Co., 403 U.S. 713 (1971).

70. United States v. Wash. Post Co., No. 71 Civ. 1235 (D.D.C. June 21, 1971), *excerpts reprinted in* THE PENTAGON PAPERS AND THE COURTS, *supra* note 31, at 98.

publication being enjoined."[71] The Supreme Court's June 25 order granting certiorari directed the government to complete the process of enumerating problematic items to supplement the Special Appendix, as the Second Circuit's order had envisioned.[72]

Under the Supreme Court's order, then, the government's case would stand or fall on the items in the Special Appendix and the supplemental list. Before oral argument on June 26, Solicitor General Erwin Griswold had apparently concluded that the government's only chance of winning the case was to narrow the range of items as to which it was seeking to restrain publication. The Solicitor General immediately conceded at oral argument that the supplemental list—filed under his signature but by necessity prepared by others—was dramatically overbroad, inasmuch as it purported to include unspecified material relating to thirteen different subjects.[73] The Solicitor General asked the Court to focus only on the items discussed in the Special Appendix filed in the Second Circuit and on eleven specific items covered in a closed brief filed in the Supreme Court.[74] The case that the government sought to make at the Supreme Court, then, was not that publication of the entire forty-seven-volume study should be enjoined, but rather that publication of a specific subset of the materials should be enjoined.[75] The secret brief emphasized two broad categories of material: material allegedly relating to *current diplomatic relations* of the United States and material relating to *current*

71. *N.Y. Times Co.*, 444 F.2d at 544. The court also ruled that on June 25, 1971, the restraining order then in place would expire as to all items not designated in the Special Appendix or the government's supplemental designation. *Id.* The effect of the court's decision was to permit the government to designate items posing a serious threat to national security. As to any items not so designated, the restraining order would automatically expire.

72. The Court's June 25 order required the government to file the Special Appendix and supplemental list by 5:00 PM that day and to serve both on the *Times* and the *Post*, even though the Special Appendix arose only in the *Times* case. *See* United States v. Wash. Post Co., 403 U.S. 943 (1971). Although the effect of the stay order was to permit publication after June 25, 1971, of any items not designated in the Special Appendix or supplemental list, uncertainty as to the scope of the supplemental list's coverage precluded publication of additional material until the Supreme Court's decision on June 30. *See* RUDENSTINE, *supra* note 3, at 264.

73. Transcript of Oral Argument, *supra* note 63, at 218-19.

74. *Id.* Solicitor General Griswold mentioned ten items in his closed brief, *id.* at 220, but it in fact contained eleven. *See* Brief for the United States (Secret Portion), N.Y. Times Co. v. United States, 403 U.S. 713 (1971) (Nos. 1873 & 1885) [hereinafter Secret Brief] (on file with author).

75. Transcript of Oral Argument, *supra* note 63, at 230 (seeking restraint "on the publication of the now quite narrowly selected group of materials covered in the special appendix, and dealt with in some detail in [the] closed brief").

military operations of the United States. As to both categories, the government claimed that further disclosure would jeopardize national security.

Of primary importance in the first category was a collection of four "negotiating" volumes—volumes that, according to the secret brief, "contain a comprehensive detailed history of the so-called negotiating track" to end the Vietnam War.[76] (In reality, the newspapers did not even possess these volumes, because Ellsberg himself had withheld them out of concern that their release would disrupt diplomatic efforts to end the war.[77]) The brief stressed the likelihood that the contents of the negotiating volumes, which included "derogatory comments about the perfidiousness of specific persons involved," would "close up channels of communication which might otherwise have some opportunity of facilitating the closing" of the war.[78] Likewise, the brief claimed that certain materials would give offense to U.S. allies or demonstrate a breach of confidence.[79] At oral argument, without referring to the specific items at issue, the parties disputed whether information that might impair current diplomatic efforts could ever cause sufficiently serious injury to the United States to warrant an injunction. Solicitor General Griswold claimed that the D.C. District Court had erred in refusing to enjoin publication despite its explicit acknowledgment that disclosure of some of the materials would affect "the conduct of delicate negotiations now in process."[80] For the government, impairment of diplomatic efforts constituted a serious and irreparable harm. Griswold also challenged the requirement that the government demonstrate that harm will occur immediately. The government's brief had argued that "in the delicate area of foreign relations frequently it is impossible to show that something would pose an 'immediate' danger to national security, even though the long-run effect upon such security would be grave and irreparable."[81] Griswold urged that the Court consider not whether harm is "immediate," but whether harm would be "irreparable."[82] Professor Alexander Bickel, arguing

76. Secret Brief, *supra* note 74, at 4.

77. *See* UNGAR, *supra* note 21, at 83-84.

78. Secret Brief, *supra* note 74, at 4-5.

79. *Id.* at 5 (item 2); *id.* at 8 (item 9). Other items relating to diplomatic relations included the full text of a cable from Llewellyn Thompson, then Ambassador to the Soviet Union, assessing the Soviet reaction to United States involvement in Vietnam. The brief claimed that release of the cable would compromise Thompson's effectiveness as a member of the delegation negotiating the Strategic Arms Limitations Treaty. *Id.* at 7 (item 8).

80. Transcript of Oral Argument, *supra* note 63, at 228 (internal quotation marks omitted).

81. Brief for the United States at 9, N.Y. Times Co. v. United States, 403 U.S. 713 (1971) (Nos. 1873 & 1885) [hereinafter Unclassified Brief].

82. Transcript of Oral Argument, *supra* note 63, at 230-31.

for the *Times*, instead claimed that impairment of diplomatic relations—including increased difficulty of negotiating with the enemy—could never support issuance of a prior restraint.[83]

The separate opinions indicated that at least some Justices were skeptical of the government's position on whether an impairment of diplomatic relations could pose a grave or immediate threat, particularly after a massive security breach was already known. For the Justices who considered this issue, one difficulty was that much harm to U.S. diplomatic interests had already been done. As Justice White put it, "The fact of a massive breakdown in security is known, access to the documents by many unauthorized people is undeniable, and the efficacy of equitable relief against these or other newspapers to avert anticipated damage is doubtful at best."[84] Similarly, Justice Stewart noted his agreement with the executive that some of the material "should not, in the national interest, be published."[85] He nevertheless found that his standard of "direct, immediate, and irreparable damage" was not met.[86] Justice Blackmun, in contrast, relied on a dissent by Judge Wilkey in the D.C. Circuit, which suggested that continued publication of the Pentagon Papers would produce great harm, defined to include "the greatly increased difficulty of negotiation with our enemies [and] the inability of our diplomats to negotiate."[87] Like Judge Wilkey, Justice Blackmun would have treated impairment of diplomatic relations as a sufficiently "direct and immediate" harm to justify injunctive relief. Other Justices were obviously more skeptical.

Concerning *current military operations*, the government's secret brief made a number of claims. First, the brief cited instances in which disclosure could reveal "continuing military plans," specifically plans developed by the Southeast Asian Treaty Organization (SEATO) to deal with contingencies in Laos, Cambodia, Thailand, and Pakistan.[88] Second, the brief claimed that portions of the study contained "names and activities of CIA agents still active

83. *Id.* at 235. Though Professor Bickel stated only that "impairment of diplomatic relations" could not provide a basis for a prior restraint, he was responding to a question quoting Judge Wilkey's statement in dissent in the D.C. Circuit focusing on "greatly increased difficulty of negotiation with our enemies, the inability of our diplomats to negotiate as honest brokers between would-be belligerents." *Id.* (quoting United States v. Wash. Post Co., 446 F.2d 1327, 1329 (D.C. Cir. 1971) (en banc) (Wilkey, J., dissenting)).

84. *N.Y. Times*, 403 U.S. at 733 (White, J., concurring).

85. *Id.* at 730 (Stewart, J., concurring).

86. *Id.*

87. *Id.* at 762 (Blackmun, J., dissenting) (quoting *Wash. Post Co.*, 446 F.2d at 1329 (Wilkey, J., dissenting)).

88. Secret Brief, *supra* note 74, at 6 (item 4).

in Southeast Asia."[89] Third, the brief asserted that certain portions of the study revealed information on intelligence estimates regarding Soviet capabilities[90] and counterintelligence successes in decrypting foreign communications.[91] The brief asserted that such information, though relating to past events, would provide other countries with insight into current U.S. intelligence and counterintelligence capabilities. At oral argument, again without referring to these specific items, the parties disputed whether the connection between the study's historical materials and current military efforts was strong enough to support a claim that public disclosure of the materials would damage national security. Alluding to the government's evidence on this subject, Professor Bickel focused on the speculative nature of the causal chain between release of the documents and the claimed national security damage. The government's claims about military matters, he argued, involved "addition of a possible cause to a train of causal factors, to a train of events that's well on the rails as is, and propelled by sufficient other factors."[92] Some Justices implicitly accepted the *Times*'s argument that disclosure must be an important cause of, not simply one of many factors contributing to, the stated danger. Justice Stewart's test, for example, asked whether disclosure "surely" would result in "direct, immediate, and irreparable damage."[93] Similarly, Justice Brennan rejected "surmise or conjecture that untoward consequences may result."[94]

Although the separate opinions do not clarify precisely what standard the government must meet to justify injunctive relief barring further disclosure, they suggest that the Justices who formed the majority required a tight causal nexus between the documents and the alleged harm. The linkages between the study's historical materials and current military operations and diplomatic efforts were not strong enough to support injunctive relief. The Court's decision also left open questions of scope and immediacy. Only Justice Brennan's opinion arguably addressed the scope of an event that would trigger injunctive relief, implying that the magnitude of the event would depend on whether the nation is at war. For peacetime suppression, his example was extreme—"information that would set in motion a nuclear holocaust."[95]

89. *Id.* at 5 (item 3).

90. *Id.* at 6 (item 5).

91. *Id.* at 8-9 (item 10).

92. Transcript of Oral Argument, *supra* note 63, at 238.

93. N.Y. Times Co. v. United States, 403 U.S. 713, 730 (1971) (Stewart, J., concurring).

94. *Id.* at 725-26 (Brennan, J., concurring).

95. *Id.* at 726.

Implicit in this discussion is the fact that the government and the newspapers had dramatically different views about what deference the courts owed to the government's claim that harm would result from disclosure of the Pentagon Papers. The government's initial position was that the classification of the materials was enough to establish harm. Although the government softened that position before the Supreme Court, its brief still emphasized that the question whether the disclosure of military secrets would result in harm "involves difficult and complex judgments which do not lend themselves to judicial resolution."[96] In the government's view, the Court should rely on the fact of classification and on the government's in camera evidence to sustain its claim that disclosure would threaten serious harm to national security. The newspapers, in contrast, emphasized the need to scrutinize the government's assertions of harm.[97] The Court implicitly rejected the government's conception of deference.

In sum, despite the seemingly straightforward conclusion that the task of balancing the public's interest in disclosure against the risks of harm fell to the newspapers, the separate opinions raise legal limits on that power: the possibility of injunctive relief in a narrow range of cases involving a showing of potential harm—a showing that could not be met by the government's mere assertions, but that was still not fully defined as to scope, immediacy, or proximity.

3. The Potential for Criminal Sanctions

Despite divisions within the Court on the availability of injunctive relief and the showing of harm required, the separate opinions also illustrate a key factual assumption shared by a number of Justices: that the newspapers would not publish material that would cause serious harm to national security interests. One possible constraint on publication was the risk of criminal sanctions. Because the United States chose to proceed against the newspapers by seeking injunctive relief rather than pursuing criminal charges, the lawsuits did not require the Court to examine the scope of the underlying federal statute, a provision of the Espionage Act of 1917, and no opinion attempted to construe the statute definitively. Nevertheless, several of the opinions reflect shared views about the power of Congress to criminalize publication of

96. Unclassified Brief, *supra* note 81, at 18.

97. *See supra* note 92 and accompanying text; *see also* Brief for the N.Y. Times Co. at 56-57, *N.Y. Times Co.*, 403 U.S. 713 (No. 1873) (arguing that in the First Amendment context, courts cannot—and do not—simply defer to the executive's decision to classify material).

harmful national security information, and the extent to which Congress had already done so.

First, a number of Justices distinguished between the power of a court to enjoin publication and the power of Congress to criminalize publication. Justice White's opinion was the most explicit on this point: "I would have no difficulty in sustaining convictions [under the Espionage Act] on facts that would not justify the intervention of equity and the imposition of a prior restraint."[98] Justice Stewart joined Justice White's opinion and referred in his own opinion to the possibility of criminal prosecution: "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."[99] Among the dissenters, both Chief Justice Burger[100] and Justice Blackmun[101] endorsed Justice White's discussion of the possibility of criminal prosecution.

Justice Marshall's opinion also discussed at length the possibility of criminal liability. For Justice Marshall, the key to the case was that Congress had, through the adoption of several criminal statutes, provided the President with "broad power to protect the Nation from disclosure of damaging state secrets."[102] The government had not shown why these statutes were inapplicable—a predicate, in Justice Marshall's view, for establishing the propriety of equitable relief in the first instance. If the government could claim in good faith that the conduct was criminal, then it could use a threat of criminal prosecution to protect the country. On the other hand, if the government could not claim in good faith that the conduct was criminal, then the executive could not invoke the Court's equitable power to "prevent behavior that Congress has specifically declined to prohibit."[103]

The point of this discussion is not to suggest that the Espionage Act in fact criminalized the conduct of the *Times* and the *Post*. I discuss the complexities of this issue in Section II.B. Rather, the opinions reveal the consensus of five Justices that Congress either could have or did criminalize the conduct—a proposition that only Justice Douglas (joined by Justice Black) explicitly

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

99. *Id.* at 730 (Stewart, J., concurring).

100. *Id.* at 752 (Burger, C.J., dissenting).

101. *Id.* at 759 (Blackmun, J., dissenting).

102. *Id.* at 743 (Marshall, J., concurring).

103. *Id.* at 742.

rejected.[104] More important than the actual reach of the Espionage Act is the premise underlying these discussions: that the threat of prosecution would shape publishers' behavior, even as to material the publishers could not be enjoined from releasing.

4. Responsible Journalism

The separate opinions in *New York Times Co. v. United States* suggest another check on the disclosure by the press of materials related to national security: the obligation of the press itself to withhold material that could cause harm. That obligation may flow from the possibility of criminal liability, from market forces (such as the anticipated advertiser or subscriber reaction to a disclosure), or from recognized journalistic norms. Justice White, joined by Justice Stewart, acknowledged the role of self-restraint by the press, backstopped by the possibility of criminal liability: "[B]ecause the material poses substantial dangers to national interests and because of the hazards of criminal sanctions, a responsible press may choose never to publish the more sensitive materials."[105] Chief Justice Burger highlighted an "approach . . . that great newspapers have in the past practiced and stated editorially to be the duty of an honorable press"[106] – to work with the government to determine whether an agreement could be reached on publication. Under this approach, the "newspapers and Government might well have narrowed the area of disagreement as to what was and was not publishable, leaving the remainder to be resolved in orderly litigation, if necessary."[107] Chief Justice Burger's position obviously differed from that of Justices White and Stewart, in that Chief Justice Burger envisioned a court serving as the arbiter of disputes between the government and the press. At bottom, however, his vision of a responsible press collaboratively weighing the national security harms that disclosure would raise was similar to that of Justices White and Stewart. Similarly, Justice Blackmun urged the newspapers to "be fully aware of their ultimate responsibilities to the United States of America," warning that if serious harm came from publication, "the Nation's people will know where the responsibility for these sad consequences rests."[108]

104. *Id.* at 721-22 (Douglas, J., concurring).

105. *Id.* at 733 (White, J., concurring).

106. *Id.* at 750 (Burger, C.J., dissenting).

107. *Id.* at 750-51.

108. *Id.* at 762-63 (Blackmun, J., dissenting).

C. Implications

The key factual dispute in the *Pentagon Papers* case was whether the government had shown that the release of the Pentagon Papers study, or even a small subset of the study, threatened sufficient harm to justify a prior restraint on its release. In holding that it did not, the Court left in the hands of the publishers the task of weighing the public interest in disclosure against the projected harm that disclosure of the Pentagon Papers would cause. The separate opinions, however, suggest divergent views about the constraints on the role of the press in publicly disclosing national security information leaked by another. At one extreme, Justices Black and Douglas left no room for executive or judicial assessment of national security harm in any case involving a leak. At the other extreme, Justice Harlan called for judicial deference to the executive's assessment of the harm the leaked materials would cause—a position that, by implication, foreclosed the possibility that the publisher would have exclusive say. Between these two extremes, a number of Justices acknowledged a point at which a court could displace a publisher's judgment with its own, although the Justices did not adopt a precise test for that point. Finally, a number of Justices presumed that the risk of criminal liability and the obligations of responsible journalism would shape the publishers' approach.

For all the differences among the separate opinions, there is one more important area of common ground. None of the opinions acknowledge the primacy of the *source*'s view of the balance of harm and public interest. Put another way, the separate opinions assumed that disclosure of national security information depends upon the judgment of the publisher—constrained by the possibility of criminal liability, by the market, or by journalistic ethics—and not solely upon the judgment of the leaker.

The next Part explores the pressures the WikiLeaks disclosures place on the *Pentagon Papers* framework.

II. THE WIKILEAKS DISCLOSURES THROUGH THE LENS OF THE PENTAGON PAPERS

At first glance, the *Pentagon Papers* case seems to map nicely on to the WikiLeaks disclosures. An anonymous source with access to classified and sensitive material, apparently disaffected with certain U.S. policies and military action that the material reveals, passes the material to an intermediary with an

infrastructure capable of disseminating the material more broadly. The U.S. government denounces the leak of the material and demands its return.[109]

If the lesson of the *Pentagon Papers* case is simply that the First Amendment fully protects the secondary transmission of leaked information, then it is difficult to see why the WikiLeaks disclosures are legally objectionable. WikiLeaks (and its media partners) stand in the shoes of the *Times* and the *Post*, with the power to assess what material ought to be disclosed. As Part I showed, however, the *Pentagon Papers* case is more complex. The Ellsberg leak shifted the power to decide what to disclose to the publishers. Yet a majority of Justices presumed that in other factual contexts, the courts would retain the power to enjoin the disclosure of information that threatened grave and imminent harm to national security. Specifically with respect to the Pentagon Papers, moreover, many Justices also anticipated that publishers within the reach of U.S. criminal law and subject to recognized journalistic norms would weigh the potential harms of disclosure against the value of public disclosure.

Assessing the WikiLeaks disclosures in light of the *Pentagon Papers* case provides an opportunity to test whether the institutional framework behind the *Pentagon Papers* case holds. I argue that it does not.

A. The WikiLeaks Disclosures

In assessing the actions of WikiLeaks, I focus mainly on the site's operation from April 2010 through the present, after it received and began processing massive amounts of material from someone with access to a closed U.S. government computer system (allegedly Private Bradley Manning, a twenty-two-year-old Army intelligence analyst[110]). Some additional background is nevertheless useful to shed light on WikiLeaks' evolution.

From its founding in 2006, WikiLeaks has attempted to serve as a clearinghouse for the dissemination of documents contributed by anonymous sources. The organization has variously characterized itself as "an uncensorable

109. *See The Defense Department's Response*, N.Y. TIMES, Oct. 22, 2010, http://www.nytimes.com/2010/10/23/world/middleeast/23response.html; Letter from Harold Hongju Koh, Legal Adviser, U.S. Dep't of State, to Jennifer Robinson, Attorney for Mr. Julian Assange, WikiLeaks (Nov. 27, 2010), *available at* http://media.washingtonpost.com/wp-srv/politics/documents/Dept_of_State_Assange_letter.pdf.

110. Ginger Thompson, *Hearing in Soldier's WikiLeaks Case Ends*, N.Y. TIMES, Dec. 22, 2011, http://www.nytimes.com/2011/12/23/us/hearing-in-private-mannings-wikileaks-case-ends.html.

Wikipedia for untraceable mass document leaking and analysis,"[111] as "a multi-jurisdictional public service designed to protect whistleblowers, journalists and activists,"[112] and as a "not-for-profit media organisation . . . bring[ing] important news and information to the public."[113] At least some of the documents WikiLeaks has released were provided to WikiLeaks through its anonymous "drop box," which WikiLeaks describes as being "fortified by cutting-edge cryptographic information technologies."[114]

Through the first four years of its existence, the site housed a range of leaked documents, including documents claimed to reveal oppression, corruption, or other scandals within foreign governments,[115] documents claimed to reveal corporate or other private wrongdoing,[116] unreleased (but unclassified) U.S. government reports,[117] and sensitive documents relating to political figures (including a collection of e-mails hacked from Sarah Palin's Yahoo! account[118] and the tightly held membership lists of the far-right British

111. *Wikileaks: About*, WIKILEAKS, http://web.archive.org/web/20070928101508/http://wikileaks.org/wiki/Wikileaks:About (last visited Aug. 24, 2011) (accessing Internet Archive from Sept. 28, 2007).

112. *Id.*

113. *About: What Is Wikileaks?*, WIKILEAKS, http://www.wikileaks.org/About.html (last visited Nov. 30, 2011).

114. *Id.* As of this writing, however, WikiLeaks' drop box for electronic submissions has been unavailable for several months. *See Submissions*, WIKILEAKS, http://www.wikileaks.org/Submissions.html (last visited Sept. 21, 2011).

115. For example, shortly before the Kenyan presidential election in 2007, WikiLeaks released a 2004 report by an international risk consultancy claiming that former Kenyan leader Daniel Arap Moi had siphoned off billions in government funds. *See, e.g.*, Xan Rice, *The Looting of Kenya*, GUARDIAN, Aug. 30, 2007, http://www.guardian.co.uk/world/2007/aug/31/kenya.topstories3.

116. For example, WikiLeaks released documents allegedly acquired from a disgruntled employee of the Cayman Islands bank Julius Baer Bank and Trust. The documents allegedly showed trust structures used for tax evasion. *See, e.g.*, Adam Liptak & Brad Stone, *Judge Shuts Down Web Site Specializing in Leaks*, N.Y. TIMES, Feb. 20, 2008, http://www.nytimes.com/2008/02/20/us/20wiki.html.

117. *See* Brian Krebs, *Thousands of Congressional Reports Now Available Online*, WASH. POST, Feb. 11, 2009, http://www.washingtonpost.com/wp-dyn/content/article/2009/02/11/AR2009021101388.html.

118. *See* Elana Schor, *Wikileaks Posts a Hack of Palin's E-mail Account*, GUARDIAN: DEADLINE USA BLOG (Sept. 18, 2008, 8:56 AM), http://www.guardian.co.uk/world/deadlineusa/2008/sep/17/uselections2008.sarahpalin.

National Party[119]). In November 2009, WikiLeaks released more than 500,000 intercepts of pager messages sent on September 11, 2001.[120]

Since early 2010, the focus on WikiLeaks has centered on its release of sensitive U.S. government materials. On April 5, 2010, the site released what has come to be known as the "Collateral Murder" video—classified military footage of three U.S. helicopter strikes in Baghdad on July 12, 2007. The strikes killed roughly a dozen people, including two Reuters war correspondents.[121] For some observers, the graphic video raised the possibility that trigger-happy U.S. soldiers mistook camera equipment for weapons; WikiLeaks decried the killings as "indiscriminate" and "unprovoked."[122] Versions of the graphic video were viewed some two million times on YouTube and replayed in hundreds of news reports.[123]

In July and October of 2010, WikiLeaks released two additional sets of materials, but under a somewhat different model. Rather than simply posting the materials on its own site, with or without comment, WikiLeaks provided the documents in advance to several Western news organizations, including the *New York Times*, the *Guardian* newspaper in London, and the German magazine *Der Spiegel*, on the condition that the papers not report on the documents until the dates on which WikiLeaks planned to release the material.[124] The July data set contained nearly 92,000 documents dating from 2004 through the end of 2009 related to the war in Afghanistan. The

119. *See* Robert Booth, *BNP Membership List Appears on Wikileaks*, GUARDIAN, Oct. 20, 2009, http://www.guardian.co.uk/politics/2009/oct/20/bnp-membership-list-wikileaks.

120. *See* Matthew Weaver, *9/11 Re-Enacted: Wikileaks Publishes September 11 Pager Messages*, GUARDIAN: NEWS BLOG (Nov. 25, 2009, 6:36 AM), http://www.guardian.co.uk/world/blog/2009/nov/25/september-11-wikileaks-pager-messages.

121. *See* COLLATERAL MURDER, http://www.collateralmurder.com (last visited Aug. 31, 2011).

122. *Id. But see* Justin Fishel, *Military Raises Questions About Credibility of Leaked Iraq Shooting Video*, FOXNEWS.COM, Apr. 10, 2010, http://www.foxnews.com/politics/2010/04/07/military-raises-questions-credibility-leaked-iraq-shooting-video/ (reporting claims that WikiLeaks selectively edited the video to emphasize the soldiers' wrongdoing). For a detailed defense of WikiLeaks' editing, see Benkler, *supra* note 14, at 322-23.

123. *See WikiLeaks Leaked Video of Civilians Killed in Baghdad—Full Video*, YOUTUBE, http://www.youtube.com/watch?v=is9sxRfU-ik (last visited Oct. 3, 2011). Assange was nevertheless disappointed at the reception the video received—a factor that would contribute to his willingness to rely on the mainstream media to release additional materials in 2010. *See* DAVID LEIGH & LUKE HARDING, WIKILEAKS: INSIDE JULIAN ASSANGE'S WAR ON SECRECY 70-71, 97, 99 (2011).

124. *See* Editor's Note, *Piecing Together the Reports, and Deciding What to Publish*, N.Y. TIMES, July 25, 2010, http://www.nytimes.com/2010/07/26/world/26editors-note.html. For an account of the negotiations that led to WikiLeaks' sharing of data, see LEIGH & HARDING, *supra* note 123, at 98-103.

documents included military incident and intelligence reports, apparently collected from the Secret Internet Protocol Router Network (SIPRNet) system used by the Department of Defense.[125]

On July 25, each news organization independently published its analysis of the materials and linked to redacted versions of some of the underlying documents. WikiLeaks, meanwhile, posted a database containing 76,911 of the documents,[126] including some in unredacted form.[127] Reports on the materials emphasized the suspicions of American soldiers on the ground that Pakistan's military has thwarted American efforts in Afghanistan by failing to cooperate in confronting Afghan insurgents and even by cooperating with insurgents themselves;[128] that a classified group of U.S. military operatives known as Task Force 373 targeted top commanders within the Afghan insurgency, with some of its operations leading to the death of civilians;[129] and that the use of drone aircraft is less effective than had been officially portrayed.[130]

The second data set, released in October 2010, included 391,832 documents,[131] also apparently collected from SIPRNet. Like the Afghan War documents, the materials consisted of military incident and intelligence reports, this time on the Iraq War. WikiLeaks made the documents available to its partners in June 2010, again on the condition that the news organizations

125. Kim Zetter, *Army: Manning Snuck 'Data-Mining' Software onto Secret Network*, WIRED: THREAT LEVEL BLOG (Apr. 4, 2011, 4:28 PM), http://www.wired.com/threatlevel/2011/04/manning-data-mining.

126. *See War Events: Index*, AFGHANWARLEAK, http://afghanwarleak.org (last visited Oct. 26, 2011) (replicating the WikiLeaks database, which contained 76,911 entries).

127. *See, e.g.*, Eric Schmitt & Charlie Savage, *U.S. Military Scrutinizes Leaks for Risks to Afghan*, N.Y. TIMES, July 28, 2010, http://www.nytimes.com/2010/07/29/world/asia/29wikileaks.html; Jeanne Whalen, *Rights Groups Join Criticism of WikiLeaks*, WALL ST. J., Aug. 9, 2010, http://online.wsj.com/article/SB10001424052748703428604575419580947722558.html. Despite not redacting the documents, WikiLeaks apparently withheld the remaining 15,000 documents out of concern that those documents, labeled "threat reports," would contain information identifying informants or those who had collaborated with U.S. forces. *See* LEIGH & HARDING, *supra* note 123, at 112.

128. Mark Mazzetti et al., *Pakistan Aids Insurgency in Afghanistan, Reports Assert*, N.Y. TIMES, July 25, 2010, http://www.nytimes.com/2010/07/26/world/asia/26isi.html.

129. *See, e.g.*, Nick Davies, *Afghanistan War Logs: Task Force 373—Special Forces Hunting Top Taliban*, GUARDIAN, July 25, 2010, http://www.guardian.co.uk/world/2010/jul/25/task-force-373-secret-afghanistan-taliban.

130. *See* C.J. Chivers et al., *View Is Bleaker than Official Portrayal of War in Afghanistan*, N.Y. TIMES, July 25, 2010, http://www.nytimes.com/2010/07/26/world/asia/26warlogs.html.

131. *The WikiLeaks Iraq War Logs: Greatest Data Leak in US Military History*, DER SPIEGEL, Oct. 22, 2010, http://www.spiegel.de/international/world/0,1518,724845,00.html; *see* Zetter, *supra* note 125.

not report on the documents until an agreed-upon release date. The release occurred on October 22, and by this time WikiLeaks had developed an automated editing program to redact names in an effort to ensure that persons identified in the reports would not be subject to reprisals.[132] Reports on the documents focused heavily on evidence of Iraqi brutality against detainees in Iraqi prisons—brutality that American military personnel were aware of but did not systematically address.[133] Other coverage focused on Iraqi civilian casualties,[134] the Iraq War's extensive reliance on private contractors,[135] and factors contributing to the success of the "surge."[136]

Perhaps the most controversial WikiLeaks data set is its cache of confidential diplomatic cables. On November 28, 2010, WikiLeaks announced that it possessed 251,287 cables originating from the State Department and 274 U.S. embassies and consulates around the world.[137] Two days earlier, Assange had contacted Louis Susman, the U.S. ambassador to the United Kingdom, inviting the United States to "privately nominate any specific instances . . . where it considers the publication of information would put individual persons at significant risk of harm."[138] Through the State Department's Legal Adviser, Harold Hongju Koh, the United States refused.[139] The U.S. government had been aware for over six months of the possibility that WikiLeaks held the cables, because Private Manning had claimed, in the online chat that ultimately led to his arrest, to have downloaded the cables from a military computer

132. *See, e.g.*, LEIGH & HARDING, *supra* note 123, at 112.

133. *See, e.g.*, Nick Davies, Jonathan Steele & David Leigh, *Iraq War Logs: Secret Files Show How US Ignored Torture*, GUARDIAN, Oct. 22, 2010, http://www.guardian.co.uk/world/2010/oct/22/iraq-war-logs-military-leaks; David Leigh & Maggie O'Kane, *Iraq War Logs: US Turned Over Captives to Iraqi Torture Squads*, GUARDIAN, Oct. 24, 2010, http://www.guardian.co.uk/world/2010/oct/24/iraq-war-logs-us-iraqi-torture.

134. *See* Sabrina Tavernise & Andrew W. Lehren, *A Grim Portrait of Civilian Deaths in Iraq*, N.Y. TIMES, Oct. 22, 2010, http://www.nytimes.com/2010/10/23/world/middleeast/23casualties.html.

135. *See, e.g.*, James Glanz & Andrew W. Lehren, *Use of Contractors Added to War's Chaos in Iraq*, N.Y. TIMES, Oct. 23, 2010, http://www.nytimes.com/2010/10/24/world/middleeast/24contractors.html.

136. *See* Sabrina Tavernise, *Mix of Trust and Despair Helped Turn Tide in Iraq*, N.Y. TIMES, Oct. 23, 2010, http://www.nytimes.com/2010/10/24/world/middleeast/24surge.html.

137. *See Secret US Embassy Cables*, WIKILEAKS, http://www.wikileaks.org/cablegate.html (last visited Sept. 21, 2011).

138. Letter from Julian Assange, Editor in Chief, WikiLeaks, to Louis B. Susman, U.S. Ambassador to the U.K., Nov. 26, 2010, *available at* http://documents.nytimes.com/letters-between-wikileaks-and-gov.

139. *See* Letter from Harold Hongju Koh to Jennifer Robinson, *supra* note 109.

system.[140] Again shifting its disclosure model, WikiLeaks did not post the entire cache of cables at once. Rather, it began by releasing 220 cables in coordination with various news organizations. This time, apparently angered by the *Times*'s refusal to link to WikiLeaks' war logs databases as well as an unfavorable front-page profile of him, Assange had not shared the cables with the *New York Times* and had extracted a promise from the *Guardian* not to do so. Upon discovering that others had copies of the cables, the *Guardian* passed them to the *Times*.[141] The *Guardian*, the *Times*, and *Der Spiegel*, along with two other newspapers that received the cables, the French paper *Le Monde* and the Spanish paper *El País*, again attempted to redact the names of individuals who spoke privately to diplomats, with the *Times* consulting the Department of State on these issues.[142] The WikiLeaks versions of the cables initially incorporated those redactions. WikiLeaks and the news organizations continued to release the cables in batches through late August of 2011, with less than 10% of the cables being released over a nine-month period.[143] Beginning on August 23, 2011, however, WikiLeaks began releasing large batches of cables in unredacted form.[144] The release was prompted by disclosure that an encrypted file available on the Internet could be decrypted by using a password that a *Guardian* reporter had revealed in a book several months earlier.[145] By September 2, WikiLeaks had released all of the remaining cables in unredacted form, both on its site and as an archive via the BitTorrent protocol.[146]

140. *See* Evan Hansen, *Manning-Lamo Chat Logs Revealed*, WIRED: THREAT LEVEL BLOG (July 13, 2011, 3:40 PM), http://www.wired.com/threatlevel/2011/07/manning-lamo-logs.

141. *See* Bill Keller, *The Boy Who Kicked the Hornet's Nest*, *in* OPEN SECRETS, *supra* note 14, at 11-12.

142. 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.

143. *See* Scott Shane, *Spread of Leaked Cables on Web Prompts Dispute*, N.Y. TIMES, Sept. 1, 2011, http://www.nytimes.com/2011/09/02/us/02wikileaks.html.

144. *See* Scott Shane, *WikiLeaks Prompts New Diplomatic Uproar*, N.Y. TIMES, Aug. 31, 2011, http://www.nytimes.com/2011/09/01/us/01wikileaks.html.

145. *See, e.g.*, James Ball, *WikiLeaks Prepares to Release Unredacted Cables*, GUARDIAN, Sept. 1, 2011, http://www.guardian.co.uk/media/2011/sep/01/wikileaks-prepares-unredacted-us-cables; *Guardian Journalist Negligently Disclosed Cablegate Passwords*, WIKILEAKS (Sept. 1, 2011), http://www.wikileaks.org/Guardian-journalist-negligently.html; *see also* LEIGH & HARDING, *supra* note 123, at 135 (using Assange's 58-character password as a chapter subheading).

146. *See Secret US Embassy Cables*, *supra* note 137 (indicating that all 251,287 cables had been released); *WikiLeaks*, TWITTER (Sept. 2, 2011, 5:12 AM EST), http://twitter.com/#!/wikileaks/status/109599482034913280 (showing the last announcement of the release of cables on WikiLeaks' site); *WikiLeaks*, TWITTER (Sept. 1, 2011, 6:53 PM EST), http://twitter.com/#!/wikileaks/status/109443867455131649 (noting the availability of the full archive via BitTorrent); *see also* CABLEGATE'S CABLES, http://www.cablegatesearch.net/search.php (last visited Oct. 31, 2011) (providing a search capability for all 251,287 cables).

B. WikiLeaks and the Presumption of "Intermediation"

Rightly or wrongly, a number of Justices in the *Pentagon Papers* case presumed publishers' intermediation of a source's unauthorized leak. The Court's holding that the government could not enjoin the release of the information meant that the press, not the government, would assess the risks of disclosure of the documents in that case. A majority of Justices recognized a stopping point at which the potential harm might be so significant as to warrant judicial intervention. In addition, a number of Justices assumed that sensitivity to the need to avoid harm (whether prompted by the possibility of criminal liability, market-related concerns, or journalistic ethics) would shape publishers' decisions. This Section considers the WikiLeaks disclosures in light of this understanding of the institutional structure for national security disclosures.

1. The Premise of Enforceability

Recall that in the *Pentagon Papers* case, seven Justices accepted the possibility that, in appropriate circumstances, the government could seek an injunction against the secondary transmission of harmful national security information. In the view of the concurring Justices, the material at issue in the Pentagon Papers study did not rise to the level required for injunctive relief. Among the Justices who left open the possibility of injunctive relief on different facts, however, there was a shared assumption that a publisher receiving and then distributing leaked national security information would be within the enforceable reach of U.S. criminal law. The *Pentagon Papers* defendants submitted to the jurisdiction of U.S. courts and indicated that they would abide by the Supreme Court's decision.[147]

The WikiLeaks disclosures raise two questions concerning the reach of U.S. law, neither of which was presented in *New York Times Co. v. United States*. The first concerns whether U.S. law can reach the extraterritorial activities of an entity like WikiLeaks – which, as noted, has relied mainly on infrastructure outside of the United States to host its site. (The actions of the mainstream media entities outside of the United States raise similar questions.) For purposes of discussion, we can assume that a provision of the Espionage Act of 1917 discussed in the *Pentagon Papers* case, 18 U.S.C. § 793(e), would apply to the dissemination of classified information by an entity like WikiLeaks, because WikiLeaks "communicates, delivers, [or] transmits" national defense

147. *See* UNGAR, *supra* note 21, at 209.

information to persons or entities not entitled to receive it.[148] (The scope of that provision, as we shall see, is more controversial than its text would suggest.) Even if WikiLeaks' conduct would fall within the scope of the statute if undertaken within the United States, does the statute extend to conduct undertaken elsewhere?

Whether a criminal prohibition such as § 793(e) applies outside the United States is primarily a question of statutory construction.[149] Courts typically apply a presumption against extraterritoriality and require a clear indication in the statute's text, structure, or legislative history that Congress intended a statute to have extraterritorial reach.[150] The Espionage Act does not contain specific language providing for extraterritorial application. Courts have recognized, however, that the presumption against extraterritoriality is weaker in cases involving alleged crimes against the U.S. government. As the Court put it in the case of *United States v. Bowman*, such crimes "are, as a class, not logically dependent on their locality for the Government's jurisdiction, but are enacted because of the right of the Government to defend itself against obstruction, or fraud wherever perpetrated, especially if committed by its own citizens, officers or agents."[151] Accordingly, the intent to reach extraterritorial conduct can be inferred from the nature of the offense.

Although *Bowman* itself involved the prosecution of U.S. citizens who committed an offense outside of the United States, courts have recognized that the right of the government to protect itself from certain harmful conduct does not logically depend on the nationality of the offender. In *United States v. Zehe*, a district court directly confronted whether a different provision of the

148. 18 U.S.C. § 793(e) (2006). There are other potentially relevant statutory provisions, including 18 U.S.C. § 641, which prohibits converting any "record, voucher, money, or thing of value of the United States" as well as receiving the same "with intent to convert it to [one's] use or gain," and 18 U.S.C. § 421(c), which prohibits disclosure of information relating to the identity of a covert agent, with intent to expose the covert agent and reason to believe that "such activities would impair or impede the foreign intelligence activities of the United States." For further discussion of these and other statutory provisions potentially bearing on national security disclosures by the press, see Steven I. Vladeck, *Inchoate Liability and the Espionage Act: The Statutory Framework and the Freedom of the Press*, 1 HARV. L. & POL'Y REV. 219, 228-31 (2007).

149. In some cases, there may be relevant constitutional limitations, including limitations on the scope of congressional power and limitations imposed by the Due Process Clause of the Fifth Amendment. In addition, limitations on jurisdiction recognized under international law may be relevant, because courts typically will not construe a congressional statute to violate international law. The former set of limitations does not apply in this context; I consider the latter set of limitations *infra* text accompanying note 158.

150. *See, e.g.*, EEOC v. Arabian Am. Oil Co., 499 U.S. 244, 258 (1991).

151. United States v. Bowman, 260 U.S. 94, 98 (1922).

Espionage Act could reach the actions of an East German citizen who allegedly committed acts of espionage in Mexico and East Germany.[152] Relying on the *Bowman* principle, the court reasoned that "espionage is an offense threatening the national security of the United States, regardless of where it occurs."[153] As the court noted, the 1948 recodification of the Espionage Act contained a provision stating that chapter 37 of Title 18 shall apply "within the admiralty and maritime jurisdiction of the United States and on the high seas, as well as within the United States."[154] In 1961, Congress repealed this provision. By virtue of its title, the repealing statute indicated Congress's purpose "to extend the application" of the espionage and censorship provisions.[155] As for whether the Act could apply extraterritorially to noncitizens as well as citizens, the court reasoned that the Act does not distinguish between citizens and noncitizens[156] and had been used to prosecute citizens and noncitizens alike before the repeal of the territorial limitation in 1961.[157] The court therefore held that the statute reached the defendant's conduct. Although *Zehe* was a classic espionage case, and the court analyzed the jurisdictional effects of the crime in that context, one could imagine a similar argument that the release of classified national security information could be harmful regardless of the location of the release or the nationality of the individual who released it. In other words, as a matter of statutory interpretation, the Espionage Act would likely reach conduct undertaken outside the United States. As a matter of customary international law, moreover, the assertion of jurisdiction over an entity operating outside of the United States would be consistent with the effects principle, under which a state has jurisdiction to enforce its laws when extraterritorial conduct has harmful effects within the state.[158]

152. United States v. Zehe, 601 F. Supp. 196, 197 (D. Mass. 1985).

153. *Id.* at 197-98.

154. *Id.* at 198 (quoting 18 U.S.C. § 791 (repealed 1961)); *see also infra* note 198 (discussing the jurisdictional provision and its repeal).

155. Act of October 4, 1961, Pub. L. No. 87-369, § 1, 75 Stat. 795, 795 (entitled "An Act to repeal section 791 of Title 18 of the United States Code so as to extend the application of chapter 37 of Title 18, relating to espionage and censorship").

156. *Zehe*, 601 F. Supp. at 200.

157. *Id.*

158. *See, e.g.*, Hartford Fire Ins. Co. v. California, 509 U.S. 764, 796 (1993) (recognizing the applicability of the Sherman Antitrust Act to "foreign conduct that was meant to produce and did in fact produce some substantial effect in the United States"); *see also* Jack L. Goldsmith, *Against Cyberanarchy*, 65 U. CHI. L. REV. 1199, 1208 (1998) (observing that customary international law permits a state "to apply its law to extraterritorial behavior with substantial local effects").

The second question the WikiLeaks disclosures present is whether any judgment rendered against WikiLeaks would be enforceable. Here, the differences between the *Times* and the *Guardian* on the one hand and WikiLeaks on the other are instructive. A judgment against the *Times* would obviously be enforceable. With respect to the *Guardian*, although it is a British newspaper, its online site reaches a substantial audience in the United States[159] and it employs a significant number of U.S.-based reporters.[160] The fact that the publisher has a substantial U.S. presence makes it more likely that a court could successfully enforce a judgment against it. Application of U.S. law to WikiLeaks, by contrast, would raise a host of legal and practical questions relating to how the United States could hale WikiLeaks into court or enforce a judgment against it. WikiLeaks has no physical U.S. presence. Nor does it substantially rely on U.S. intermediaries to sustain its technical infrastructure. After the first batch of diplomatic cables was released, WikiLeaks hosted the cables on servers located in France.[161] When hackers launched distributed denial of service (DDoS) attacks against WikiLeaks' main page, Assange moved the WikiLeaks' main page to Amazon's commercial hosting service, and Amazon's servers were able to withstand the DDoS attacks.[162] Amazon soon refused to continue hosting WikiLeaks' pages,[163] and WikiLeaks moved its pages to a redundant network of foreign servers, including some held in a military-style bunker in Sweden.[164] Thus, even if the materials WikiLeaks planned to disclose contained information that could have caused grave, immediate harm to national security, thereby satisfying the standard that some Justices in the *Pentagon Papers* assumed could justify injunctive relief, it is difficult to see how the United States could have enforced an injunction against a far-flung web of redundant servers before the information was disseminated.[165]

159. *See, e.g.*, LEIGH & HARDING, *supra* note 123, at 202 (noting that in the wake of the cables' release, roughly 43% of the hits on the *Guardian*'s online WikiLeaks coverage came from the United States).

160. *See Guardian in America: Meet the Team*, GUARDIAN, Sept. 14, 2011, http://www.guardian.co.uk/help/2011/sep/14/guardian-us-staff-list.

161. LEIGH & HARDING, *supra* note 123, at 204.

162. *Id.*

163. *Id.* at 205.

164. Andy Greenberg, *Wikileaks Servers Move to Underground Nuclear Bunker*, FORBES, Aug. 30, 2010, http://www.forbes.com/sites/andygreenberg/2010/08/30/wikileaks-servers-move-to-underground-nuclear-bunker.

165. *Cf.* Bambauer, *supra* note 7, at 35 (noting that WikiLeaks "has . . . proved considerably immune to legal efforts to interdict its operations").

That is not to say that the United States would lack tools for an ex post response to unlawful disclosures. The point for now is that whatever force the Espionage Act might exert ex ante upon U.S. media entities or others with a significant U.S. presence to avoid publishing information that would cause grave, immediate harm, it does not necessarily shape or constrain WikiLeaks' actions in the same way.

2. The Premise of Criminal Liability

In the *Pentagon Papers* case, the United States had invoked the Espionage Act of 1917 as the basis for its suits against the *Times* and the *Post*. Because it considered only the propriety of the government's request for injunctive relief, the Court had no need to consider fully whether the disclosure of harmful national security information would subject the *Times* and the *Post* to ex post criminal liability. A number of Justices, however, assumed that even though injunctive relief was unavailable, the newspapers publishing the study would be operating in the shadow of federal criminal law. The underlying premise of this discussion was that the government's ability to impose liability ex post was not simply a mirror image of its ability to prevent publication ex ante. Rather, the government could punish a publisher for secondary transmission of material it could not enjoin. Does that assumption continue to hold, with respect to news organizations generally and with respect to WikiLeaks? Answering this question requires assessment both of the substantive scope of the Espionage Act and of how the First Amendment constrains operation of the statute.

a. Substantive Scope of the Espionage Act

In their seminal article on the Espionage Act of 1917, Professors Harold Edgar and Benno Schmidt wrote that since World War I, we have lived in a state of "benign indeterminacy" about the legal rules governing publication of national security information.[166] The crux of the problem, they explain, is that despite a legislative history that "may fairly be read as excluding criminal sanctions for well-meaning publication of national security information," the language of the Espionage Act has to be "bent" to exclude such publication from the statute's reach.[167] The United States has not vigorously pursued

166. Harold Edgar & Benno C. Schmidt, Jr., *The Espionage Statutes and Publication of Defense Information*, 73 COLUM. L. REV. 929, 936 (1973).

167. *Id.* at 937.

prosecution of downstream disclosures of national security information, instead seeking to identify and punish the leaker.[168] The Espionage Act remains on the books, however, and government officials continue to assert that,[169] while scholars and other commentators continue to debate whether,[170] the statute provides a viable alternative for punishing the downstream disclosure of national security information. In assessing how the statute might apply to publication of national security information, it is useful to separate two questions: (1) whether the statute applies at all outside the context of classic espionage; and (2) if so, whether it extends to downstream publication of leaked national security information.

Broadly speaking, the Espionage Act prohibits a range of conduct with respect to information connected with the national defense. Section 794(a) of Title 18 of the U.S. Code, which derived from § 2(a) of the 1917 Act, prohibits classic espionage—the communication, delivery, or transmission of national defense information to a foreign government or representative thereof "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 a foreign nation."[171] Similarly, § 794(b), the successor to § 2(b) of the 1917 statute, prohibits collecting, recording, publishing, or communicating defense plans "with intent that the same shall be communicated to the enemy."[172] Section 793 of Title 18 also contains a number of other provisions on the handling of information relating to the national defense. More specifically, § 793 prohibits entering a U.S.-owned or U.S.-controlled protected place to obtain certain national defense

168. *See, e.g.*, *Espionage Act and the Legal and Constitutional Issues Raised by WikiLeaks: Hearing Before the H. Comm. on the Judiciary*, 111th Cong. 17 (2010) [hereinafter Constitutional Issues Hearing] (prepared statement of Prof. Geoffrey R. Stone, University of Chicago Law School) [hereinafter Stone Judiciary Statement]; William H. Freivogel, *Publishing National Security Secrets: The Case for "Benign Indeterminacy,"* 3 J. NAT'L SEC. L. & POL'Y 95, 96 (2009).

169. *See, e.g.*, Dianne Feinstein, Op-Ed., *Prosecute Assange Under the Espionage Act*, WALL. ST. J., Dec. 7, 2010, http://online.wsj.com/article/SB10001424052748703989004575653280626335258.html; *see also* Letter from Harold Hongju Koh to Jennifer Robinson, *supra* note 109 (citing ongoing violation of law).

170. For a selection of views, see Constitutional Issues Hearing, *supra* note 168 (statements and testimony of Thomas S. Blanton, Director, National Security Archive, George Washington University; Abbe David Lowell, Partner, McDermott Will & Emery, LLP; Professor Geoffrey R. Stone, University of Chicago Law School; Dr. Gabriel Schoenfeld, Senior Fellow, Hudson Institute; Kenneth L. Wainstain, Partner, O'Melveny & Myers, LLP; and Professor Stephen I. Vladeck, American University).

171. 18 U.S.C. § 794(a) (2006).

172. *Id.* § 794(b).

information;[173] gathering without authority material connected with the national defense;[174] receiving such material knowing it to have been improperly obtained;[175] communicating without authority such material to one not entitled to receive it;[176] failing to deliver such material to an appropriate government official;[177] and negligently causing loss of such information.[178]

For present purposes, § 793(d)-(e) are the most relevant provisions of the statute. Both cover one who "willfully communicates, delivers, [or] transmits" certain information concerning the national defense "to any person not entitled to receive it."[179] Before 1950, a single subsection, 18 U.S.C. § 793(d), had covered the transmission of national defense materials. In 1950, Congress split the prohibition on transmitting national defense information into two separate subsections.[180] Whereas the prior version covered transmission by one who "lawfully or unlawfully" had possession of the relevant material, the 1950 version created separate prohibitions for transmission by one who "lawfully" had possession (§ 793(d)) and transmission by one who had "unauthorized" possession (§ 793(e)). For present purposes, we can assume that WikiLeaks and its media partners had "unauthorized" possession of national defense material.

Regarding the first question—that is, whether § 793(e) reaches disclosures unconnected to espionage—the statutory text, as many observers have noted, is broad.[181] The statute requires only a showing that the defendant transmitted information to one not entitled to receive it, not a showing that the defendant sought to place information in the hands of a foreign government. The structure of the Espionage Act as a whole confirms that reading. Each version of the statute has contained distinct prohibitions on classic espionage and on other activities connected with the handling of national defense information. Current § 794(a) prohibits the transmission of national defense information to "any foreign government, or to any faction or party or military or naval force within a foreign country, whether recognized or unrecognized by the United

173. *Id.* § 793(a).

174. *Id.* § 793(b).

175. *Id.* § 793(c).

176. *Id.* § 793(d)-(e).

177. *Id.*

178. *Id.* § 793(f).

179. *Id.* § 793(d)-(e).

180. *Id.*

181. *See, e.g.*, Edgar & Schmidt, *supra* note 166, at 1033; Vladeck, *supra* note 148, at 223.

States, or to any representative . . . thereof."[182] As noted above, current § 793, by contrast, covers a range of activities that could be preparatory to or independent of classic espionage.[183] The current structure carries forward a division between classic espionage and other offenses that first appeared in the Defense Secrets Act of 1911,[184] the precursor to the Espionage Act. In the Defense Secrets Act, section 1 covered several activities relating to the handling of national defense information, including entering a protected place to obtain national defense information or gathering, receiving, or communicating such information.[185] Section 2 of the Act set forth the punishment for one who communicated or attempted to communicate certain national defense information—"any document, sketch, photograph, photographic negative, plan, model, or knowledge" connected with the national defense—"to any foreign government, or to any agent or employee thereof."[186] The Espionage Act of 1917[187] and its major amendments[188] retained this structure.

One distinction between the Defense Secrets Act of 1911 and the Espionage Act of 1917 was that the Defense Secrets Act required proof that one who provided information to a foreign government also committed one of the acts covered in the separate prohibition on the handling of national defense information. That is, the prohibition in section 2 of the Defense Secrets Act on communicating national defense information to a foreign government required as a predicate a violation of section 1 on entering a protected place to obtain national defense information or gathering, receiving, or communicating such information.[189] Although the Defense Secrets Act thus linked classic espionage and certain preparatory acts, it required proof of the preparatory acts for an espionage conviction, not evidence of espionage to support conviction for the

182. 18 U.S.C. § 794(a).

183. *See supra* notes 173-178 and accompanying text.

184. Act of Mar. 3, 1911 (Defense Secrets Act), ch. 226, 36 Stat. 1084 (repealed by the Espionage Act of 1917, ch. 30, 40 Stat. 217).

185. *Id.* § 1, 36 Stat. at 1084-85.

186. *Id.* § 2, 36 Stat. at 1085.

187. *See* Espionage Act of 1917, ch. 30, §§ 1-2(a), 40 Stat. 217-18.

188. *See* Subversive Activities Control Act of 1950, ch. 1024, § 18, 64 Stat. 987, 1003-04 (codified as amended at 18 U.S.C. § 793 (2006)) (splitting former § 793(d)'s prohibition on transmitting national defense information into separate paragraphs for lawful and unlawful possession and adding a prohibition on failure to report loss of national defense information); Act of June 25, 1948, ch. 645, §§ 791-797, 62 Stat. 683, 736-38 (reenacting Espionage Act as 18 U.S.C. §§ 791-794). For discussion of other amendments to the 1917 Act, see *infra* note 198 and accompanying text.

189. Defense Secrets Act, ch. 266, § 2, 36 Stat. at 1085.

preparatory acts. In any event, the Espionage Act of 1917 eliminated the Defense Secrets Act's linkage between classic espionage acts and the remaining statutory prohibitions. As a result, the government has on numerous occasions prosecuted classic spying under both § 794(a), which requires a showing that the defendant transferred information to a foreign government, and under § 793(d)-(e), which require only a showing that the defendant transferred information to one not entitled to receive it.[190] In *United States v. Morison*, for example, the Court of Appeals for the Fourth Circuit confirmed that § 793(d)-(e) are substantially broader than §794(a): "[S]ection 794 covers 'classic spying'; sections 793(d) and (e) cover a much lesser offense . . . and extend[] to disclosure to *any* person 'not entitled to receive' the information."[191]

The conclusion that § 793(e) of Title 18 reaches more than acts preparatory to espionage does not resolve whether the provision extends to publication. The statute, as noted, covers one who "communicates, delivers, [or] transmits" certain information. Although the text of § 793(e) may be broad enough to include publication, a number of surrounding statutory provisions do specifically prohibit publication. Section 794(b), for example, covers one who "collects, records, *publishes*, or communicates" defense plans "with intent that the same shall be communicated to the enemy."[192] Section 797 covers one who "reproduces, *publishes*, sells, or gives away" images of defense installations or equipment.[193] Section 798 covers one who "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," certain classified information.[194] In the *Times* case, the district court relied in part on these surrounding provisions to conclude that Congress intended § 793(e) to exclude publication.[195]

190. *See, e.g.*, United States v. Truong Dinh Hung, 629 F.2d 908, 917-19 (4th Cir. 1980) (upholding conviction under §§ 794(a), 793(c), and 793(e)); United States v. Kampiles, 609 F.2d 1233, 1249 (7th Cir. 1979) (upholding conviction under §§ 794(a) and 793(e)); United States v. Boyce, 594 F.2d 1246, 1251 (9th Cir. 1979) (upholding conviction under § 794(a) and unspecified subsection of § 793); *see also* United States v. Morison, 844 F.2d 1057, 1067 (4th Cir. 1988) (discussing cases involving prosecution under both § 794(a) and § 793(d)-(e)).

191. *Morison*, 844 F.2d at 1065.

192. 18 U.S.C. § 794(b) (emphasis added).

193. *Id.* § 797 (emphasis added).

194. *Id.* § 798(a) (emphasis added). The covered classified information includes information concerning cryptographic and communications intelligence activities of the United States or any foreign government. *Id.*

195. United States v. N.Y. Times Co., 328 F. Supp. 324, 329-30 (S.D.N.Y.), *rev'd*, 444 F.2d 544 (2d Cir.) (in banc), *rev'd*, 403 U.S. 713 (1971) (per curiam)

As a matter of statutory interpretation, however, the issue is more complex. Applying the maxim *expressio unius est exclusio alterius*, courts sometimes conclude that the enumeration of some items implies exclusion of others.[196] As applied here, that maxim might lead one to conclude that § 793(e) excludes publication. Likewise, inclusion of a phrase in one portion of a statute and its omission in another may give rise to an inference that Congress intended to exclude it where omitted.[197] Section 793(e), however, is a poor candidate for application of these interpretive principles. Of the three surrounding provisions that contain the word "publishes," two came from statutes other than the Espionage Act. Within Chapter 37 of Title 18 of the U.S. Code, §§ 792-794 derive from the Espionage Act, which was adopted two months after the United States declared war on Germany and last significantly amended in 1950.[198] These provisions appear alongside provisions from two entirely separate statutes.[199] First, in 1938, Congress passed a "censorship" statute prohibiting the dissemination of images of defense installations or equipment.[200] The censorship statute, now codified at 18 U.S.C. §§ 795-797,

196. *See, e.g.*, Block v. Cmty. Nutrition Inst., 467 U.S. 340, 349 (1984); Nat'l R.R. Passenger Corp. v. Nat'l Ass'n of R.R. Passengers, 414 U.S. 453, 458 (1974).

197. *See, e.g.*, Keene Corp. v. United States, 508 U.S. 200, 208 (1993); Russello v. United States, 464 U.S. 16, 23 (1983) ("[W]here Congress includes particular language in one section of a statute but omits it in another section of the same Act, it is generally presumed that Congress acts intentionally and purposely in the disparate inclusion or exclusion." (quoting United States v. Wong Kim Bo, 472 F.2d 720, 722 (5th Cir. 1972) (alteration in original))).

198. Espionage Act of 1917, ch. 30, 40 Stat. 217 (codified as amended at 18 U.S.C. §§ 792-794 (2006)). As discussed *supra* note 188, Congress reenacted the Espionage Act's provisions in 1948 as 18 U.S.C. §§ 791-795, as part of the general revision and recodification of the federal criminal code. *See* Act of June 25, 1948, ch. 645, §§ 791-797, 62 Stat. 683, 736-38. In 1950, Congress rewrote § 793, creating separate offenses for transmission of national defense information, depending on whether the defendant had lawful or unlawful possession of the information. *See* 18 U.S.C. § 793(d)-(e). Congress also amended the Espionage Act in 1961 to repeal 18 U.S.C. § 791, which had stated that Chapter 37 of Title 18 shall apply "within the admiralty and maritime jurisdiction of the United States and on the high seas, as well as within the United States." *See* Act of Oct. 4, 1961, Pub. L. No. 87-369, § 1, 75 Stat. 795, 795. The effect of the repeal was to permit extraterritorial application of the espionage and censorship provisions. *See supra* notes 154-155 and accompanying text. Other nontechnical amendments after 1950 involved punishment rather than the statute's substantive scope. *See* Espionage and Sabotage Act of 1954, Pub. L. No. 777, ch. 1261, § 201, 68 Stat. 1216, 1219 (codified at 18 U.S.C. § 794) (increasing the punishment for peacetime espionage to include the death penalty; allowing punishment for any term of years or life in wartime or peacetime); *see also* Omnibus Diplomatic Security and Antiterrorism Act of 1986, Pub. L. No. 99-399, § 1306, 100 Stat. 853, 898 (codified at 18 U.S.C. §§ 793(h), 794(d)) (providing for forfeiture of proceeds derived from espionage activities).

199. *See supra* text accompanying notes 171-178.

200. Act of Jan. 12, 1938, ch. 2, 52 Stat. 3, 3-4 (codified as amended at 18 U.S.C. §§ 795-797).

allows the President to designate defense-related installations and equipment to be protected[201] and makes it unlawful for any person to reproduce, publish, sell, or give away images of such installations or equipment without permission, unless the images bear an indication that they have been "censored" by the proper military authorities.[202] Second, in 1951, Congress added a prohibition on transmission of certain types of classified information.[203] That provision, codified at 18 U.S.C. § 798, provides for punishment of one who "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," classified information concerning cryptographic and communications intelligence activities of the United States or any foreign government.[204]

Chapter 37 of Title 18 of the U.S. Code, then, is a collection of three statutes from three different eras—1917, 1938, and 1951. In 1948, Congress re-codified in a single chapter the Espionage Act of 1917 and the 1938 "censorship" statute covering images of defense installations and equipment,[205] with an important amendment to the former to follow in 1950.[206] In 1951, Congress added the provisions on the dissemination of classified information concerning cryptographic systems and communications intelligence.[207] Thus, although §§ 797 and 798 contain references to publishing, they were not part of the Espionage Act, and the language that Congress ultimately included in § 793(e) well predated the adoption of these statutes. These provisions therefore have limited bearing upon construction of § 793(e).[208]

Section 794(b)'s prohibition on collecting, recording, publishing or communicating defense plans may be more pertinent, because it derived from section 2(b) of the Espionage Act of 1917 and was thus enacted at the same time

201. 18 U.S.C. § 795.

202. *Id.* § 797.

203. Act of Oct. 31, 1951, ch. 655, § 24, 65 Stat. 710, 719-20 (codified as amended at 18 U.S.C. § 798).

204. 18 U.S.C. § 798(a).

205. Act of June 25, 1948, ch. 645, §§ 791-797, 62 Stat. 683, 736-38.

206. Subversive Activities Control Act of 1950, ch. 1024, § 18, 64 Stat. 987, 1003-04 (amending 18 U.S.C. § 793 (1950)).

207. Act of Oct. 31, 1951, ch. 655, § 24(a), 65 Stat. 710, 719-20 (codified at 18 U.S.C. § 798).

208. Some scholars nevertheless refer to the surrounding provisions as part of the Espionage Act. *See, e.g.*, Vladeck, *supra* note 148, at 225 (categorizing §§ 797 and 798 as "provisions of the Espionage Act").

as other Espionage Act provisions that did not contain the word "publishes," including section 1(d), the precursor to the current § 793(d)-(e). Still, it is unclear that the use of the word "publishes" in section 2(b) of the Espionage Act should lead to an inference that publication is excluded from other provisions. Section 2(b) was new to the Espionage Act in 1917,[209] whereas the other sections of the Act had been drawn from the Defense Secrets Act of 1911.[210] Sections 1 and 2 of the Defense Secrets Act each covered one who "communicates [national defense information] to" a third party—to "any person not entitled to receive it," in the case of section 1, and to a foreign government, in the case of section 2.[211] In the Espionage Act, Congress expanded these provisions. Section 1(d) covered one who "communicates *or transmits*" national defense information and section 2(a) covered one who "communicates, *delivers, or transmits*" such information.[212] This modification suggests that Congress intended to enlarge rather than contract the scope of each provision. Section 2(b) of the Espionage Act, moreover, was structurally dissimilar to the provisions drawn from the Defense Secrets Act, inasmuch as section 2(b) covered both the collection and the dissemination of defense plans[213]—actions that, with respect to national defense information, were treated in different subsections of section 1 of the Espionage Act.[214] In other words, it is difficult to infer that the addition of a new prohibition on gathering and transmitting defense plans should be construed to narrow the separate prohibition on conveying the broader category of national defense information to those not entitled to receive it.[215]

209. Espionage Act of 1917, ch. 30, § 2(b), 40 Stat. 217, 218-19 (codified as amended at 18 U.S.C. §§ 792-799).

210. *See supra* notes 184-186 and accompanying text.

211. Defense Secrets Act, ch. 226, §§ 1-2, 36 Stat. 1084, 1084-85 (1911).

212. Espionage Act §§ 1(d), 2(a), 40 Stat. at 218 (emphases added). The omission of "delivers" from § 1(d) of the Espionage Act persisted until the 1950 amendment. *See* Subversive Activities Control Act of 1950, ch. 1024, § 18, 64 Stat. 987, 1004 (amending 18 U.S.C. § 793 (1950)).

213. Espionage Act § 2(b), 40 Stat. at 218-19 (covering whoever "shall collect, record, publish, or communicate").

214. Espionage Act § 1(b), (d), 40 Stat. at 218 (separately covering the gathering of material connected with the national defense and the transmission of such material).

215. *Cf.* Edgar & Schmidt, *supra* note 166, at 1035 (noting that the use of the word "publish" in section 2(b) "makes clear the draftsmen's intent that it be covered in [that] newly drafted section[], but the failure to use the term in the carried-over subsections 1(d) and 2(a) does not prove the converse"). Section 1(d) of the Espionage Act persisted until the 1950 amendment. *See* Subversive Activities Control Act, § 18, 64 Stat. at 1004.

A final argument that the statute excludes publication comes not from the text but from the legislative history of the Espionage Act of 1917. One of the early drafts of the statute provided that the President could, by proclamation, prohibit the publication of "information relating to the national defense which, in his judgment, is of such character that it might be useful to the enemy."[216] In his concurrence in the *Pentagon Papers* case, Justice Douglas noted that the congressional debates leading to the defeat of this measure included discussion of the First Amendment.[217] Aside from the fact that it is difficult to discern *why* Congress rejected this provision,[218] an interpretation of the statute that excludes publication, but not other forms of communication, creates a significant anomaly, in that publication to a wide audience may well be more harmful than other methods of communication.[219] I discuss in Part III other statutory elements that may narrow the Espionage Act's prohibition on communications. For now, however, I proceed on the assumption that the phrase "communicates, delivers, [or] transmits" includes publication, and I consider how the First Amendment bears on the provision's reach.

b. First Amendment Considerations

As discussed earlier, the *Pentagon Papers* case suggests a narrow range of circumstances in which the government might be entitled to injunctive relief prohibiting the publication of national security information—as, for example, when publication would carry the risk of grave and irreparable damage to the United States.[220] The question is whether, in light of the First Amendment, the standard for criminal punishment ex post is broader than or the same as the standard for enjoining release of the information ex ante. This question has both doctrinal and normative dimensions.

As a doctrinal matter, cases decided after the *Pentagon Papers* case shed some light on, but do not resolve, the issue. The Supreme Court, for example, has invalidated state attempts to impose civil or criminal penalties on the publication of lawfully obtained, truthful information, over assertions that the penalties were necessary to safeguard certain state interests. A trilogy of cases

216. 55 CONG. REC. 1763 (1917) (proposed section 4).

217. New York Times Co. v. United States, 403 U.S. 713, 721-22 (1971) (Douglas, J., concurring).

218. *See* Edgar & Schmidt, *supra* note 166, at 941 (noting that "it is often debatable whether solicitude for freedom of the press or political anxiety about the powers of a war-time President led Congress to resist broad prohibitions on publication").

219. *See id.* at 1035-36.

220. *See supra* Subsection I.B.2.

involving privacy interests is illustrative. In *Cox Broadcasting Corp. v. Cohn*, for example, the Court vacated a civil damages award against a television station that broadcast the name of a rape-murder victim after obtaining the name from court records.[221] In *Smith v. Daily Mail Publishing Co.*, the Court held that a state could not prosecute newspapers for violating a state statute that prohibited newspapers (but not other media entities) from disclosing the name of a juvenile offender, where the newspaper obtained the name through routine reporting techniques.[222] Finally, in *Florida Star v. B.J.F.*, the Court invalidated a civil damages award against a newspaper that published the name of a rape victim after obtaining the name from a police department incident report, which had included the name inadvertently and in violation of state law.[223] The Court's approach in these cases is well captured in *Daily Mail Publishing*: "[I]f 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."[224] Importantly, however, the Court in these cases did not adopt a categorical rule that truthful publication may never be punished consistent with the First Amendment. As the Court put it in *Florida Star*, "Our cases have carefully eschewed reaching this ultimate question, mindful that the future may bring scenarios which prudence counsels our not resolving anticipatorily."[225] In addition, the Court explicitly avoided opining on whether a different result would follow if either the newspaper or the source had obtained the information *unlawfully*.[226]

221. 420 U.S. 469 (1975).

222. 443 U.S. 97 (1979).

223. 491 U.S. 524 (1989).

224. *Daily Mail Publ'g Co.*, 443 U.S. at 103. Beyond the trilogy discussed in the case, see *Landmark Communications, Inc. v. Virginia*, 435 U.S. 829 (1978), in which the Court invalidated the application to a newspaper of a Virginia statute prohibiting one from divulging information from proceedings of state judicial review commissions, where the information was secured by legal means.

225. *Fla. Star*, 491 U.S. at 532; *see also Landmark Commc'ns*, 435 U.S. at 838 (rejecting the contention that "truthful reporting about public officials in connection with their public duties is always insulated from the imposition of criminal sanctions by the First Amendment," and finding it "unnecessary to adopt this categorical approach to resolve the issue before us").

226. *See Fla. Star*, 491 U.S. at 535 n.8 (noting that the Court had not yet settled the issue whether, "in cases where the 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").

More recently, in *Bartnicki v. Vopper*, the Court considered whether the First Amendment shields the disclosure of information that a publisher knows or has reason to know was unlawfully obtained by its source.[227] *Bartnicki* involved the interception of a cell phone call between the president of and chief negotiator for a teacher's union, concerning contentious collective bargaining negotiations between the union and the local school board. An unknown third party intercepted the call and provided the tape to a union opponent, who in turn provided it to a local radio commentator, who played the tape over the air. Section 2511(1)(c) of the Federal Wiretap Act prohibits one from disclosing a communication that he or she knows or has reason to know was obtained through an illegal interception.[228] For purposes of considering the constitutionality of the statute, the Supreme Court assumed that the radio commentator knew or should have known that the conversation was illegally intercepted.[229] That assumption brought the commentator's conduct squarely within the ambit of § 2511(1)(c) and raised the question whether the First Amendment immunized that conduct.

The Court first recognized that the government must have a "need . . . of the highest order" to justify punishing the publication of truthful information.[230] The Court considered two possible justifications: "the interest in removing an incentive for parties to intercept private conversations" and "the interest in minimizing harm to persons whose conversations have been illegally intercepted."[231] The Court found the deterrence rationale wholly unpersuasive: "[I]t 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."[232] If current sanctions on illegal interception are insufficient, the Court reasoned, Congress could increase them, and there was little evidence that the difficulty in identifying those who illegally intercept communications justified punishing disclosure to eliminate the market for illegal interception. The Court found the interest in minimizing harm to the victim of the interception to be much more significant: "[T]here is a valid independent justification for prohibiting . . . disclosures by persons who lawfully obtained access to the contents of an illegally intercepted message, even if that prohibition does not play a significant role in preventing such

227. 532 U.S. 514 (2001).

228. *See* 18 U.S.C. § 2511(1)(c) (2006).

229. *Bartnicki*, 532 U.S. at 525.

230. *Id.* at 528 (quoting Smith v. Daily Mail Publ'g Co., 443 U.S. 97, 103 (1979)).

231. *Id.* at 529.

232. *Id.* at 529-30.

interceptions from occurring in the first place."[233] On the facts of the case, however, the Court concluded that the disclosure prohibition could not be enforced. The communications at issue related to a debate about matters of unquestionable public interest. In such a case, the Court reasoned, § 2511(1)(c)'s disclosure prohibition "implicates the core purposes of the First Amendment because it imposes sanctions on the publication of truthful information of public concern."[234] Drawing upon the classic principle that "[t]he right of privacy does not prohibit any publication of matter which is of public or general interest," the Court ruled that the privacy considerations had to give way.[235]

Bartnicki, while instructive, does not squarely resolve when Congress can constitutionally punish the publication of harmful national defense information. Section 793(e)'s prohibition on disclosure of national defense information, like the prohibition in § 2511(1)(c) on illegally intercepted communications, almost certainly sweeps in truthful information of high public value. The *Bartnicki* Court, however, did not hold that the First Amendment always immunizes such conduct. Rather, the Court concluded that privacy concerns could not trump the First Amendment's protection of speech about a matter of public concern. The Court's fact-specific approach leaves open the question of when, if ever, national security harms might trump that protection. In addition, the *Bartnicki* Court, like the *Florida Star* Court, emphasized that the party *receiving* the information had not acted unlawfully. The structure of the Espionage Act creates an additional twist. The Wiretap Act prohibited the party who unlawfully intercepted the communication from disclosing or using it, but did not prohibit its *receipt*.[236] In *Florida Star*, the Court noted that the state had not prohibited the receipt of information concerning a victim of sexual assault. In contrast to the provisions at issue in those cases, 18 U.S.C. § 793(c) does prohibit receiving national defense information, knowing that it has been obtained in violation of the Espionage Act.[237] *Bartnicki* holds that the First Amendment shields the disclosure of information of public concern when the party disclosing it obtained it *lawfully*, not when the party disclosing it received it *unlawfully*.

233. *Id.* at 533.

234. *Id.* at 533-34.

235. *Id.* at 534 (quoting Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 214 (1890)).

236. 18 U.S.C. § 2511(1)(c) (2006).

237. 18 U.S.C. § 793(c).

In short, current doctrine does not resolve whether the assumption of some *Pentagon Papers* Justices—that the government can punish ex post what it cannot stop the press from publishing ex ante—is valid. The relevant normative considerations cut in different directions. On the one hand, if the government's interest is in preventing disclosure of information that is harmful (but not so harmful as to trigger the possibility of injunctive relief), punishment does not serve that interest once the information has been disseminated. Indeed, that is the logic of the privacy trilogy discussed above. On the other hand, the fear of criminal liability may prompt the intermediary's more careful scrutiny of the potential harm of the information in relation to the public interest.

As this discussion suggests, the assumption of a number of the *Pentagon Papers* Justices—that the threat of criminal liability for publishing material whose disclosure could not be enjoined would constrain a publisher's handling of national security information—may not hold. The Justices' analysis of this issue in the *Pentagon Papers* case was itself incomplete. Subsequent cases, particularly *Bartnicki*, suggest but do not compel the conclusion that courts should not apply dramatically different standards to evaluate the availability of a prior restraint and the availability of ex post punishment. The limited possibility of criminal liability has obvious implications for the "who decides" question, for it softens the threat of criminal liability as a constraint on how media entities evaluate the possibility of harm, except where the threat of harm is exceptionally grave.

3. The Premise of Media Self-Censorship

Finally, as discussed in Part I, a number of the *Pentagon Papers* Justices believed not only that the publishers would operate in the shadow of potential criminal liability, but that responsible journalism would shape the publishers' approaches. The separate opinions presumed that the publishers would not operate in disregard of the potential harm the disclosure would cause. Rather, they would carefully scrutinize the materials and assess the potential for harm prior to publication.

Testing the extent to which this premise held in the case of the WikiLeaks disclosures is exceedingly difficult, because the disclosures involved multiple media outlets with different markets and sensibilities. There is unquestionably evidence of the media carefully scrutinizing and redacting the material

WikiLeaks supplied.[238] One could argue that WikiLeaks' decision to "launder" the leaked information through the mainstream media ensured that the materials would be scrubbed for harmful information.[239] The picture is somewhat more complicated, however. In the war log and diplomatic cable releases, WikiLeaks acted both as a publisher and as an information broker, and these roles deserve distinct treatment. Likewise, WikiLeaks published a great deal more information than did its media partners, thus requiring different treatment of WikiLeaks and the remaining publishers.

a. WikiLeaks as Publisher

As noted earlier, WikiLeaks has functioned in part as a secure repository for anonymously leaked information. As the "wiki" in its name suggests, WikiLeaks was originally founded on a collaborative model. WikiLeaks encouraged outsiders to process and analyze information available on the site for the benefit of the public.[240] Although WikiLeaks soon abandoned (at least temporarily) its reliance on *user* editing and analysis of documents on its site, the site has always offered some analytical material as well as primary documents. WikiLeaks' release of the "Collateral Murder" video demonstrates the site's effort to be taken seriously by and as part of the media: the release

238. With each set of materials, the *Times* consulted U.S. officials concerning what they intended to release and redacted certain information from the documents. *See* Keller, *supra* note 141, at 1, 9 ("We had approached the White House days before [the scheduled release of articles on the Afghan War logs] to get its reaction to the huge breach of secrecy as well as to specific articles we planned to write . . . ."); *id.* at 12 (describing the "early warning" given to the White House nine days before the release of the diplomatic cables); Alan Rusbridger, *Introduction* to LEIGH & HARDING, *supra* note 123, at 1, 8 (noting that the *Times* approached U.S. officials before each successive round of publication).

239. In the case of the war logs, the publishers removed names to protect the identities of persons who had cooperated with the United States. In the initial cable releases in late 2010, the publishers likewise redacted from the cables the names of informants and persons who consulted with U.S. diplomats. *See* LEIGH & HARDING, *supra* note 123, at 110-12; Keller, *supra* note 141, at 8. The U.S. government, meanwhile, claimed that it had worked to notify—and in some cases even relocate—individuals whose names did or could appear. *See* Mark Landler & Scott Shane, *U.S. Sends Warning to People Named in Cable Leaks*, N.Y. TIMES, Jan. 6, 2011, http://www.nytimes.com/2011/01/07/world/07wiki.html; Peter Walker, *WikiLeaks Cables Prompt US To Move Diplomatic Sources*, GUARDIAN, Jan. 7, 2011, http://www.guardian.co.uk/world/2011/jan/07/wikileaks-cables-us-diplomatic-sources.

240. *See Wikileaks: About*, *supra* note 111 ("In place of a couple of academic specialists, Wikileaks provides a forum for the entire global community to examine any document relentlessly for credibility, plausibility, veracity and validity. The global community is able to interpret documents and explain their relevance to the public.").

occurred at the National Press Club, where Assange commented on the video extensively.[241]

With the war log and diplomatic cable disclosures, WikiLeaks' approach to redaction and the withholding of information shifted over time. The media entities with which WikiLeaks shared its databases culled through the information and published a small selection of the materials in redacted form. For the war logs, WikiLeaks released much more than its media partners—76,911 documents of roughly 92,000 it claimed to have in its database. The 15,000 unreleased documents were "threat reports" that appeared to present a greater risk of mentioning names of informants or those who had collaborated with coalition forces.[242] WikiLeaks later developed software to strip names and key details from the documents and deployed this program to redact the Iraq War logs before posting that database.[243] WikiLeaks' slow release of the diplomatic cables—after the U.S. government rebuffed WikiLeaks' request to identify specific materials that would place individuals at risk—permitted it to mirror the redactions of its media partners, until the compromise of the password to a version of the cables database available on the Internet prompted the release of the full trove of unredacted cables.

The evidence on WikiLeaks' efforts to forestall harm that the release of the materials could bring is mixed. Journalists who worked with WikiLeaks claimed that initially Assange was philosophically opposed to redaction; they were able to convince him that inclusion of information on informants or collaborators would delegitimize the entire project.[244] When it became clear that a password to the leaked cables had been compromised, however, WikiLeaks abandoned its redaction efforts—after conducting a Twitter poll on whether to release the cables in redacted or unredacted form.[245]

b. WikiLeaks as Information Broker

WikiLeaks' role as information broker presents additional difficulties. WikiLeaks began its disclosures in partnership with the *New York Times*, the *Guardian*, and *Der Spiegel*, with *Le Monde* and *El País* joining the project

241. *See* Raffi Khatchadourian, *No Secrets: Julian Assange's Mission for Total Transparency*, NEW YORKER, June 7, 2010, http://www.newyorker.com/reporting/2010/06/07/100607fa_fact_khatchadourian.

242. *See supra* note 127.

243. LEIGH & HARDING, *supra* note 123, at 112.

244. *Id.* at 110-12.

245. Ball, *supra* note 145.

later.[246] Each publisher portrayed itself as being ethically committed to avoiding harm by redacting information that could endanger informants or reveal sensitive intelligence methods.[247] The publishers nevertheless took different positions on whether to consult the U.S. government about impending disclosures. The *Times*, for example, shared information on the diplomatic cables it intended to print, whereas the *Guardian* shared only the order of countries whose cables it intended to cover.[248]

For some observers, the extent of the *Times*'s consultation indicates insufficient distance between the *Times* and the government. Statements by the *Times* in connection with this and prior disclosures, if taken at face value, suggest both an ethical obligation to avoid harm and a healthy skepticism for government claims of harm. The *Times* certainly attempts to portray its decisions to publish sensitive information as being fully informed by national security considerations, but balanced against its obligation to disclose matters of public importance. In June 2006, for example, the *New York Times*, *Los Angeles Times*, and *Wall Street Journal* each disclosed the existence of a secret arrangement between the United States and the Society for Worldwide Interbank Financial Telecommunication (SWIFT), a consortium of financial institutions that runs a worldwide communications network carrying instructions for international transfers of money and securities.[249] Under this arrangement, the Treasury Department issued administrative subpoenas on a monthly basis for disclosure of a subset of SWIFT records. Those records then became part of a database that U.S. analysts could search for terrorism-related connections.[250] The disclosures prompted sustained criticism, particularly of the *New York Times*, on the ground that disclosure of the program alerted terrorists to U.S. investigative tools. *Times* Executive Editor Bill Keller noted that Administration officials asked the *Times* not to reveal the program, saying that the disclosure could jeopardize the program's effectiveness—because the

246. *See supra* text accompanying notes 124 and 142.

247. *See supra* notes 238-239 and accompanying text.

248. LEIGH & HARDING, *supra* note 123, at 188-90.

249. Eric Lichtblau & James Risen, *Bank Data Is Sifted by U.S. in Secret To Block Terror*, N.Y. TIMES, June 23, 2006, http://www.nytimes.com/2006/06/23/washington/23intel.html; Josh Meyer & Greg Miller, *U.S. Secretly Tracks Global Bank Data*, L.A. TIMES, June 23, 2006, http://articles.latimes.com/2006/jun/23/nation/na-swift23; Glenn R. Simpson, *Treasury Tracks Financial Data in Secret Program*, WALL ST. J., June 23, 2006, http://online.wsj.com/article/SB115101988281688182.html.

250. *See The Terror Financial Tracking Program: Hearing Before the Subcomm. on Oversight and Investigations of the H. Comm. on Fin. Servs.*, 109th Cong. 27 (2006) (statement of Stuart Levey, Under Sec'y, Terrorism and Financial Intelligence, U.S. Dep't of the Treasury).

SWIFT consortium would withdraw its cooperation, or because terrorists would change their tactics.[251] A week after the disclosures, the *Wall Street Journal*'s editorial page recounted that the Secretary of the Treasury, the co-chairs of the 9/11 Commission, Democratic Congressman John Murtha, and Director of National Intelligence John Negroponte had also asked the *Times* not to reveal the information.[252] The *Times*'s public editor eventually wrote that the disclosure was improper—that in the absence of evidence of illegality or abuse, the *Times* should not have published an article disclosing the program.[253]

In an op-ed published after the decision to run the SWIFT story, Keller and the editor of the *L.A. Times*, Dean Baquet, observed that publishers are indeed sensitive to U.S. officials' concerns:

> No article on a classified program gets published until the responsible officials have been given a fair opportunity to comment. And if they want to argue that publication represents a danger to national security, we put things on hold and give them a respectful hearing. . . . Finally, we weigh the merits of publishing against the risks of publishing. . . . [M]aking those decisions is the responsibility that falls to editors, a corollary to the great gift of our independence. It is not a responsibility we take lightly. And it is not one we can surrender to the government.[254]

This approach to the SWIFT disclosures is consistent with what a number of Justices assumed was at work in the *Pentagon Papers* case, even if some might question whether the editors properly weighed the relevant considerations. WikiLeaks' role as information broker, however, complicates matters.

The fact that WikiLeaks brokered the materials to different media partners made it difficult for any one of the entities to engage in self-censorship based on concerns about potential harms of disclosure. By way of comparison, the *New York Times* delayed its publication of a story on the Bush Administration's

251. *Letter from Bill Keller on the Times's Banking Records Report*, N.Y. TIMES, June 25, 2006, http://www.nytimes.com/2006/06/25/business/media/25keller-letter.html; Lichtblau & Risen, *supra* note 249.

252. *See* Editorial, *Fit and Unfit To Print*, WALL ST. J., June 30, 2006, http://online.wsj.com/article_email/SB115163079557294963-lMyQjAxMDE2NTMxMDYzMzAwWj.html.

253. *See* Byron Calame, *Can 'Magazines' of the* Times *Subsidize News Coverage?*, N.Y. TIMES, Oct. 22, 2006, http://www.nytimes.com/2006/10/22/opinion/22pubed.html.

254. Dean Baquet & Bill Keller, Op-Ed., *When Do We Publish a Secret?*, N.Y. TIMES, July 1, 2006, http://www.nytimes.com/2006/07/01/opinion/01keller.html.

warrantless eavesdropping program for more than a year.[255] According to *Times* Executive Editor Bill Keller, the delay was influenced by the Bush Administration's objections that publication would compromise ongoing antiterror operations and that the initial reporting did not accurately convey the level of oversight to which the program was subject.[256] The *Times* could not possibly have attempted this sort of delay with the WikiLeaks disclosures.[257]

Even if the publishers that partnered with WikiLeaks were sensitive to the national security interests at stake in the war log and cable disclosures, one can reasonably ask whether other entities with less significant U.S. connections would take the same guarded approach to the materials. Indeed, it is noteworthy that the *Guardian* reporter who first approached Assange concerning the sharing of the databases proposed adding other partners for the purpose of jurisdictional arbitrage. The *Guardian* favored inclusion of the *New York Times* in the releases because the *Guardian* would be less likely to face an effort under British law to enjoin publication if the *New York Times* published the materials as well.[258] In other words, the *Guardian* could leverage the global media marketplace to enable itself to publish more than its domestic law might otherwise allow.

The involvement of multiple media partners in the WikiLeaks disclosures no doubt fueled some healthy competition among the publishers. There are a

255. Calame, *supra* note 253; James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES, Dec. 16, 2005, http://www.nytimes.com/2005/12/16/politics/16program.html. For other examples of press self-censorship prompted by concerns over the national security ramifications of disclosure, see Mary-Rose Papandrea, *The Publication of National Security Information in the Digital Age*, 5 J. NAT'L SEC. L. & POL'Y 119, 121 (2011).

256. *Talk to the Newsroom: Executive Editor Bill Keller*, N.Y. TIMES, Apr. 14, 2006, http://www.nytimes.com/2006/04/14/business/media/14asktheeditors.html; *see also* Byron Calame, *Behind the Eavesdropping Story, a Loud Silence*, N.Y. TIMES, Jan. 1, 2006, http://www.nytimes.com/2006/01/01/opinion/01publiceditor.html (criticizing the failure of *Times* editors to explain the publication delay more fully); Byron Calame, *Eavesdropping and the Election: An Answer on the Question of Timing*, N.Y. TIMES, Aug. 13, 2006, http://www.nytimes.com/2006/08/13/opinion/13pubed.html (discussing the length of the publication delay in relation to the 2004 presidential election).

257. For a similar assessment, see Benkler, *supra* note 14, at 349 (noting that WikiLeaks' decision to release materials through several established news sites in different markets and jurisdictions created "enough competition to prevent any organization from deciding, in the name of responsibility, not to publish at all, or . . . to delay publication").

258. *See* LEIGH & HARDING, *supra* note 123, at 97, 100 (noting the view of the *Guardian*'s Nick Davies, who brokered the deal with Assange, that simultaneous publication of the material in several countries, including in the United States by the *Times*, might stave off the threat of a British injunction); Keller, *supra* note 141, at 11 (stating that the *Guardian* included the *Times* in part because "given the potential legal issues and public criticism it was good to have company in the trenches").

number of ways in which foreign coverage of specific documents or issues differed significantly from coverage within the United States. To take one example, the Afghan War logs included dozens of documents involving Task Force 373, a joint team of elite special operations forces with a "capture/kill" list of Taliban and Al Qaeda targets.[259] Among other things, the documents describe accidental civilian deaths at the hands of the unit. In one June 2007 incident, a team hunting alleged Taliban commander Qari Ur-Rahman engaged in a firefight and called for air support, only to discover that it had been engaged with Afghan National Police officers, seven of whom were killed and four of whom were wounded.[260] In a second incident approximately a week later, a team targeted Al Qaeda member Abu Laith al-Libi, who was believed to be running terrorist training camps in the border region with Pakistan. The team fired five rockets at a compound in Paktika Province where al-Libi was believed to be hiding. The attack killed six Taliban insurgents but also killed seven children inside an Islamic school.[261]

The *New York Times*, the *Guardian*, and *Der Spiegel* each discussed revelations about Task Force 373 in their opening packages of articles on the Afghan War logs. In the *Times*, however, Task Force 373 received a single bullet point, with the *Times* describing the unit as a "secret commando unit[]" working from a list of "about 70 top insurgent commanders."[262] The missions, the *Times* noted, "claim notable successes, but have sometimes gone wrong, killing civilians and stoking Afghan resentment."[263] The *Guardian* and *Der Spiegel* ran much more extensive analyses of incidents involving the unit and offered higher estimates of the number of individuals on the capture/kill list.[264]

259. *See, e.g.*, Davies, *supra* note 129; Matthias Gebauer et al., *Task Force 373 and Targeted Assassinations: US Elite Unit Could Create Political Fallout for Berlin*, DER SPIEGEL, July 26, 2010, http://www.spiegel.de/international/germany/0,1518,708407,00.html.

260. *See Afghanistan War Logs: US Special Forces Gunship Shoots 15 Police*, GUARDIAN, July 25, 2010, http://www.guardian.co.uk/world/afghanistan/warlogs/35C17E54-C611-4F39-8C39-553F5927AC96.

261. *See Afghanistan War Logs: Special Ops Squad Assault Compound and Kill Seven Children*, GUARDIAN, July 25, 2010, http://www.guardian.co.uk/world/afghanistan/warlogs/15A27543-B022-4736-AC31-71006B18794E.

262. Chivers et al., *supra* note 130.

263. *Id.*

264. The secret list is referred to as the "Joint Prioritized Effects List" (JPEL). Although the full list is not available among the Afghan War logs, various media entities have extrapolated from numbers assigned to the targets that the list includes more than 2000 people. *See* Davies, *supra* note 259; *see also* Matthias Gebauer, *The Truth About Task Force 373: War Logs Cast Light on Dirty Side of Afghanistan Conflict*, DER SPIEGEL, July 26, 2010, http://www.spiegel.de/international/world/0,1518,708559,00.html ("It is not possible to

Der Spiegel's coverage emphasized the fact that the unit's missions consisted of "targeted killings" or "targeted extermination attack[s]."[265] For the *Guardian*, the main focus of the story was the extent to which coalition press reports provided misleading information about civilian casualties inflicted by the unit.[266] In the incident involving the Afghan police officers, for example, a coalition press release noted that a firefight had occurred, but did not mention that Afghan police officers had been killed or wounded. In the incident involving the children, a coalition press statement acknowledged the deaths, but made no mention of the nature of the mission, or of the fact that the unit had fired rockets without being fired upon.[267] The Iraq War logs and the diplomatic cables provide similar examples of variances in coverage or emphasis.[268]

The range of coverage may serve the public well, by making it less likely that the government will suppress information of high public value. Just as a diversity of views on the importance of particular leaked information has the potential to expose more information of public interest, however, a diversity of views about the risks that particular information presents has the potential to expose more harmful material.

C. Implications

What lessons does *New York Times Co. v. United States* offer for the WikiLeaks disclosures, and what lessons do the WikiLeaks disclosures offer for

work out from the documents exactly how many JPEL targets there are in Afghanistan, but the four-digit process numbers are enough to suggest that the total number of targets is large.").

265. Gebauer et al., *supra* note 259.

266. Davies, *supra* note 129.

267. *Id.*

268. The *Times*'s coverage of the Iraq War logs, for example, placed less emphasis than foreign coverage on allegations that the United States, by official policy, ignored the torture of detainees by Iraqi armed forces and police—and in some cases turned detainees over to an Iraqi special forces unit known to engage in torture. *Compare, e.g.*, Sabrina Tavernise & Andrew W. Lehren, *Detainees Fared Worse in Iraqi Hands, Logs Say*, N.Y. TIMES, Oct. 22, 2010, http://www.nytimes.com/2010/10/23/world/middleeast/23detainees.html, *with* Leigh & O'Kane, *supra* note 133, *and* Davies et al., *supra* note 133. Similarly, media critics noted that the *Guardian* provided far more aggressive coverage of a directive issued under Hillary Clinton's name requiring diplomats and other State Department personnel overseas to increase their intelligence gathering activities, including by collecting information on U.N. Secretary General Ban Ki-moon. *See, e.g.*, Joel Meares, *Spy vs. Spy:* Times *and* Guardian *Differ on WikiLeaks "Spying" Revelations*, COLUM. JOURNALISM REV., Nov. 29, 2010, http://www.cjr.org/campaign_desk/spy_vs_spy.php (discussing the differences between the *Times*'s and the *Guardian*'s coverage).

New York Times Co. v. United States? For some observers, the facts of the WikiLeaks disclosures closely track the release of the Pentagon Papers, and the Pentagon Papers analogy vindicates the actions of the source and of WikiLeaks. Upon closer inspection, the picture is more complicated, because the WikiLeaks disclosures call into question key premises of some of the opinions in the *Pentagon Papers* case. First, the *New York Times* and the *Washington Post* were within the prescriptive and enforcement jurisdiction of the United States. Even if WikiLeaks' initial media partners were as well, it is not clear that a court could enforce a judgment against WikiLeaks. Second, to the extent that a majority of Justices envisioned that the threat of criminal liability would constrain national security disclosures in circumstances in which injunctive relief was unavailable, the statutory and constitutional issues are uncertain. That is, ex post liability for disclosure of harmful national security information may simply mirror the narrow circumstances in which a publisher is susceptible to injunctive relief ex ante. Finally, as for whether publishers handling leaked information draw upon an identified set of ethical precepts to balance the interest in disclosure against the potential for harm, the evidence is mixed. Assange's commitment to the redaction process waxed and waned: WikiLeaks withheld a category of Afghan documents perceived to present a heightened risk of harm, used an automated redaction program to sanitize the Iraq War logs, and relied upon its media partners' editing of the diplomatic cables.[269] WikiLeaks abandoned redaction of the cables altogether, however, once the security of a file containing the cables was compromised. WikiLeaks' media partners recognized that the legitimacy of the entire project depended on responsible treatment of the materials. At the same time, the global, fragmented media market permitted jurisdictional arbitrage. WikiLeaks' partners had different sensibilities about particular materials, and the result was likely publication of more national security information than a single media partner would have revealed. Moreover, as relations between Assange and his original partners became more strained, WikiLeaks simply turned to new ones.

In sum, the WikiLeaks disclosures illustrate significant shifts in the institutional framework for disclosing leaked national security information. The next Part considers whether these shifts demand a response.

269. *See supra* text accompanying note 143.

III. WHO DECIDES?

The Pentagon Papers analogy is so powerful for WikiLeaks defenders because it points to an instance in which, in the view of most observers, the press got the assessments of public interest and harm right: the public release of the Pentagon Papers study provided important confirmation of missteps in the Vietnam conflict and of suspicion that America's leaders had misled the public in key respects. Even Erwin Griswold, who argued on behalf of the government that the release of the items enumerated in the government's secret brief would cause irreparable damage to the United States, eventually came to the view that the disclosures had not caused the anticipated harm.[270]

Some observers have likewise argued that the anticipated harms from the WikiLeaks disclosures have not materialized. U.S. officials uniformly condemned the initial war log and diplomatic cable releases.[271] After the release of the Afghan War logs, Admiral Mike Mullen, Chairman of the Joint Chiefs of Staff, went so far as to say that those operating WikiLeaks "might already have on their hands the blood of some young soldier or that of an Afghan family."[272] Some of the concerns stemmed from the possibility that the disclosures would reveal sensitive U.S. intelligence and counterintelligence methods. Weeks after the release of the Afghan War logs, however, even Secretary of Defense Robert Gates observed that the documents had revealed no sensitive intelligence methods.[273] Other concerns stemmed from the possibility that the release of unredacted versions of some of the Afghan War logs would endanger individuals who had cooperated with coalition forces.[274] The wholesale release of the unredacted diplomatic cables in late summer 2011 raised similar concerns

270. Erwin N. Griswold, Op-Ed., *Secrets Not Worth Keeping: The Courts and Classified Information*, WASH. POST, Feb. 15, 1989, at A25 ("I have never seen any trace of a threat to the national security from the publication. Indeed, I have never seen it even suggested that there was such an actual threat. . . . There may be some basis for short-term classification while plans are being made, or negotiations are going on, but apart from details of weapons systems, there is very rarely any real risk to current national security from the publication of facts relating to transactions in the past, even the fairly recent past.").

271. *See supra* note 109 (citing sources).

272. Greg Jaffe & Joshua Partlow, *Joint Chiefs Chairman Mullen: WikiLeaks Release Endangers Troops, Afghans*, WASH. POST, July 30, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/07/29/AR2010072904900.html.

273. *See, e.g.*, Elisabeth Bumiller, *Gates Weighs Afghanistan and Leaks*, N.Y. TIMES, Oct. 16, 2010, http://www.nytimes.com/2010/10/17/world/asia/17gates.html.

274. *See supra* note 127 and accompanying text.

that some who had spoken with U.S. officials would be endangered. Commentators continue to debate whether any such fears have been realized.[275]

The issue, however, is not simply whether assessments of public interest and harm in the WikiLeaks disclosures were right or wrong. The issue, rather, is whose assessment should prevail. The *Pentagon Papers* case assured that, once information of high public value was in the hands of the press, the press's assessment would prevail over the government's, absent a showing of an extraordinary risk of harm. That case was decided against the backdrop of presumptions about the amenability of publishers to judicial process, the possibility of criminal liability, and the influence of journalistic norms. In other words, the *Pentagon Papers* case removed one control on publication of national security information—ex ante enforcement of the executive's perspective on the possibility of harm. The Court's holding did not weaken the availability of other possible controls, including media self-censorship and the possibility of ex post criminal liability. Far from fitting into the *Pentagon Papers* framework for national security disclosures, the WikiLeaks disclosures point to its instability.

The challenge raised by an unauthorized leak of national security information is that the answer to the institutional question—who decides how to balance the risks of disclosure against the benefits?—cannot simply be the source of the leak. Ellsberg's actions in conveying the Pentagon Papers to the *New York Times* are often cast as a courageous effort to expose wrongful government conduct. Whether that account is correct, and whether similar narratives about Bradley Manning are correct, we cannot assume that all releases of national security information will be benign in motivation or result. In other words, as much as a regime for national security information must account for acts of courage or patriotism in exposing wrongdoing, it must also account for the malicious, disgruntled, or misguided insider who seeks to override judgments about national security and harm made within the framework established by Congress and the executive. In his concurring opinion in *United States v. Morison*, an Espionage Act case, Judge Wilkinson aptly captured this difficulty:

275. *See, e.g.*, Bradley Klapper & Cassandra Vinograd, *AP Review Finds No Threatened WikiLeaks Sources*, HOUS. CHRON., Sept. 11, 2011, http://www.chron.com/news/article/AP-review-finds-no-WikiLeaks-sources-threatened-2164076.php; Mark MacKinnon, *Leaked Cables Spark Witch-Hunt for Chinese 'Rats,'* GLOBE & MAIL (Toronto), Sept. 14, 2011, http://www.theglobeandmail.com/news/world/asia-pacific/leaked-cables-spark-witch-hunt-for-chinese-rats/article2165339; *Ethiopian Journalist ID'd in WikiLeaks Cable Flees Country*, COMM. TO PROTECT JOURNALISTS (Sept. 14, 2011, 5:01 PM), http://www.cpj.org/2011/09/ethiopian-journalist-idd-in-wikileaks-cable-flees.php.

> To reverse Morison's conviction . . . would be tantamount to a judicial declaration that the government may never use criminal penalties to secure the confidentiality of intelligence information. . . . [T]his course would install every government worker with access to classified information as a veritable satrap. Vital decisions and expensive programs set into motion by elected representatives would be subject to summary derailment at the pleasure of one disgruntled employee. The question, however, is not one of motives as much as who, finally, must decide. The answer has to be the Congress and those accountable to the Chief Executive.[276]

The flip side of the accountability problem Judge Wilkinson mentions is that secrecy to some degree undermines accountability, for the public cannot call its officials to account on the basis of information of which it is unaware.

How should we reconcile these competing interests? Part II's assessment of the WikiLeaks disclosures demonstrates the limits of relying on publishers to moderate questions of harm and public benefit. This Part briefly considers three possibilities for rebuilding an institutional framework for mediating questions of harm and public benefit that unauthorized leaks present: revisiting the constraints on publishers' secondary transmission; relying on nonpublisher intermediaries to constrain secondary transmission; and shaping the environment for unauthorized leaks.

A. Revisiting Constraints on Publishers

As discussed in Part I, once national security information moves from the hands of an unauthorized leaker into the hands of a potential publisher, the government's judgment that disclosure will harm U.S. national security interests can be overridden by a publisher's assessment in most circumstances. The *Pentagon Papers* case foreclosed injunctive relief to prevent further disclosure of national security information, at least absent a showing that disclosure would cause grave and immediate harm. Justice Black and Justice Douglas would have held that injunctive relief to block publication is never available, and Justice Brennan's position was not a great distance from that categorical approach. The remaining Justices, however, acknowledged the possibility of injunctive relief in narrow circumstances.

In light of that acknowledgment, we can ask whether the law provides an adequate basis for the government to secure injunctive relief in the narrow

276. United States v. Morison, 844 F.2d 1057, 1083 (4th Cir. 1988).

situation the *Pentagon Papers* case preserved. As noted earlier, the *Pentagon Papers* case provided no clear demarcation for the standard under which a court can grant such relief. To date, *United States v. Progressive*, a case involving an injunction prohibiting the *Progressive* magazine from publishing certain technical information about the construction of nuclear weapons, remains the sole instance in which a court granted injunctive relief prohibiting publication based on a claim that disclosure threatened national security.[277]

In light of the questions about whether the Espionage Act reaches publication and the separation-of-powers concerns some Justices raised in the *Pentagon Papers* case, a stronger statutory basis for injunctive relief would be appropriate. The "clear and present danger" test is a possible benchmark against which to measure such a statute.[278] That test to some degree addresses the questions of scope, immediacy, and proximity the *Pentagon Papers* case raises. A revised statute, for example, could authorize the executive to seek injunctive relief barring disclosure of certain information based on a reasonable belief that disclosure would proximately cause serious bodily injury or destruction of or irreparable damage to equipment or facilities necessary to the defense of the United States or its allies. One question that this approach would raise concerns the scope or magnitude of the harm a disclosure would cause. Recall that Justice Brennan, tracking the discussion in *Near*, focused on disclosure of troop movements in a time of war; for peacetime, his example was an event akin to a nuclear holocaust. During oral argument in the *Pentagon Papers* case, Justice Stewart pointedly put the issue of scope to Professor Bickel, representing the *Times*, who conceded that the projected harm from a disclosure need not be of a "cosmic" nature to trigger injunctive relief.[279] By this logic, injunctive relief to protect diplomatic relations would not qualify, but injunctive relief to prevent a disclosure that would be the proximate cause of death or bodily injury to an informant might well qualify.

It is important to acknowledge that such a statute may not be effective in cases involving intermediaries that lack a U.S. presence. As discussed in Part II, the WikiLeaks disclosures suggest that there will be circumstances in which the legal tools to prevent downstream disclosure simply will not work. Although that fact does not lead to the conclusion that it is not worth providing a statutory avenue for such relief, it does point to the need to rely more heavily

277. United States v. Progressive, Inc., 467 F. Supp. 990 (W.D. Wis.), *dismissed*, No. 79-1428, 610 F.2d 819 (Table) (7th Cir. Oct. 1, 1979).

278. *See, e.g.*, Stone Judiciary Statement, *supra* note 168, at 20; Benkler, *supra* note 14, at 353-54.

279. *See supra* note 63.

on legal tools that shape the environment for leaks than those that control downstream disclosure.

Tools to address ex post the secondary transmission of leaked information are, by definition, less effective. The threat of criminal penalties may have some deterrent effect, at least for entities within the reach of U.S. enforcement jurisdiction. As discussed in Part II, the Espionage Act presents statutory and constitutional uncertainty. It is unclear whether the statute reaches secondary transmission of leaked material. Assuming that Congress could correct any statutory defect to clarify that it does reach publication, the question is whether applying the statute to punish publication would be constitutional—that is, does the First Amendment permit Congress to criminalize speech that it cannot constitutionally authorize a court to enjoin? Or does the same test for justifying a prior restraint also apply to punishment after the fact? There are two doctrinal distinctions between a revised 18 U.S.C. § 793(e), on the one hand, and the *Cox Broadcasting*, *Daily Mail*, and *Florida Star* trilogy as well as *Bartnicki*, on the other. First, federal law purports to make the mere receipt of national defense information a crime. The privacy trilogy preserved the question of whether the result would be different in a case involving illegal conduct by the publisher or source, and *Bartnicki* involved a recipient who presumably had reason to know that his source acted illegally but who did not himself acquire the information unlawfully. Second, and perhaps more significantly, the interests weighed against the disclosures in the *Cox Broadcasting*, *Daily Mail*, and *Florida Star* trilogy and in *Bartnicki* were individual privacy interests that, the Court found, had to give way in the face of the publication of truthful and newsworthy information. The countervailing interest in cases involving a disclosure of potentially harmful national security information seems more significant, depending on how that interest is formulated. Obviously, the closer the formulation comes to the harms that would support injunctive relief, the more likely a court would find the statute constitutional.

Although it may be possible for Congress to set the terms for injunctive relief in the case of a clear and present danger (or grave and immediate harm) to national security interests, and to clarify criminal liability for secondary transmission of leaked information, such measures may not be effective against all potential publishers or information brokers. The next Section considers the possible role of nonpublisher intermediaries in controlling secondary transmission of leaked information.

B. Nonpublisher Intermediaries

The previous Section demonstrated the limited tools in the government's toolbox to shape publishers' secondary transmission of leaked information. As many scholars have observed, the fact that Internet publishers must rely on other private parties for various services provides an attractive point of control for the government and others to shape behavior.[280] The release of the war logs and diplomatic cables offers a fascinating opportunity to examine governmental and nongovernmental interventions to thwart and support WikiLeaks, and to consider the possibilities for nonpublisher intermediaries to influence secondary transmission of leaked materials.

In the wake of the release of the diplomatic cables, WikiLeaks was subject to distributed denial of service (DDoS) attacks. Although, "the Jester," a self-described "hacktivist for good," took credit for disabling the WikiLeaks site in retaliation for WikiLeaks "attempting to endanger the lives of our troops, 'other assets' & foreign relations,"[281] there is reason to be skeptical of his claims.[282] In any event, after the attacks, Assange diverted the site's main page, WikiLeaks.org, to Amazon's commercial hosting service. Amazon soon became the first service provider to withdraw its services from WikiLeaks.[283] EveryDNS, which operated a domain name server carrying information necessary for users to connect to WikiLeaks' servers, followed suit, configuring its equipment not to respond with the IP address of WikiLeaks' servers.[284] MasterCard, Visa, and PayPal all ceased processing payments on WikiLeaks' behalf.[285]

The initial DDoS attack and the service providers' responses sparked a battle between opponents and supporters of WikiLeaks. A loosely organized

280. *See, e.g.*, Michael D. Birnhack & Niva Elkin-Koren, *The Invisible Handshake: The Reemergence of the State in the Digital Environment*, 8 VA. J.L. & TECH. 6 (2003); Joel R. Reidenberg, *States and Internet Enforcement*, 1 U. OTTAWA L. & TECH. J. 213, 222 (2003); Jonathan Zittrain, *Internet Points of Control*, 44 B.C. L. REV. 653, 660-64 (2003).

281. LEIGH & HARDING, *supra* note 123, at 204 (quoting alleged tweets of "The Jester," known as th3j35t3r).

282. *See* Benkler, *supra* note 14, at 338-39.

283. *See* Note Explaining WikiLeaks' Violation of Terms of Service, AMAZON WEB SERVICES, http://aws.amazon.com/message/65348 (last visited July 28, 2011).

284. Charles Arthur & Josh Halliday, *WikiLeaks Fights To Stay Online After US Company Withdraws Domain Name*, GUARDIAN, Dec. 3, 2010, http://www.guardian.co.uk/media/blog/2010/dec/03/wikileaks-knocked-off-net-dns-everydns.

285. Declan McCullagh, *MasterCard Pulls Plug on WikiLeaks Payments*, CNET NEWS, Dec. 6, 2010, http://news.cnet.com/8301-31921_3-20024776-281.html.

collection of hackers labeled "Anonymous" retaliated by launching attacks against the entities that had terminated services to WikiLeaks.[286] Two aspects of these postdisclosure dynamics require more discussion. The first question is whether responses of this sort are likely to be effective in curbing disclosures. The initial DDoS was effective in disabling the WikiLeaks site, but only temporarily. As for the infrastructure providers, WikiLeaks has thus far withstood the hosting service and DNS withdrawals by shifting to other hosting services and domain name servers. The withdrawal of the payment services appears to have had much more significant influence.[287]

The second question is whether such responses are legitimate. The DDoS attacks, whether pro-WikiLeaks or anti-WikiLeaks, are almost certainly unlawful in the United States.[288] As for the service withdrawals, the service providers and payment processors cited terms-of-service violations as the basis for the withdrawals. There was, however, an obvious "push" by government officials to secure the service providers' cooperation. Senator Joe Lieberman, chairman of the Senate's Committee on Homeland Security and Governmental Affairs, reportedly asked Amazon to cut off service to WikiLeaks.[289] After Amazon did so, Senator Lieberman called "on any other company or organization that is hosting WikiLeaks to immediately terminate its relationship with them."[290] If the First Amendment or related issues would prevent the government from using the judicial process to shut down a site involved in secondary transmissions of national security information, is it legitimate for government officials, even in informal or uncoordinated ways, to seek the assistance of a service provider to achieve the same outcomes? Even if the service providers responded to government pressure, the question is whether the government's requests for service withdrawals differ in any significant way from government requests for media entities to defer or withhold publication of information claimed to be sensitive. Requests to a publisher are no more transparent. Such negotiations take place out of the

286. LEIGH & HARDING, *supra* note 123, at 207-08.

287. John F. Burns, *Founder Says WikiLeaks, Starved of Cash, May Close*, N.Y. TIMES, Oct. 24, 2011, http://www.nytimes.com/2011/10/25/world/europe/blocks-on-wikileaks-donations-may-force-its-end-julian-assange-warns.html.

288. In the United States, such attacks would violate 18 U.S.C. § 1030(a)(5)(A) (2006 & Supp. III 2010).

289. Lance Whitney, *Amazon Cuts off WikiLeaks*, CNET NEWS, Dec. 2, 2010) http://news.cnet.com/8301-13578_3-20024376-38.html.

290. Ewen MacAskill, *WikiLeaks Website Pulled by Amazon After US Political Pressure*, GUARDIAN, Dec. 1, 2010, http://www.guardian.co.uk/media/2010/dec/01/wikileaks-website-cables-servers-amazon.

public eye, unless publication prompts their disclosure. One possible objection, however, is that the service providers may be more deferential to government judgments about potential national security harms than media entities might be. Put another way, neither the law nor a well-established set of intermediary ethics govern the circumstances in which a service provider can withdraw service. Although there are counterexamples illustrating heightened efforts by service providers to bring greater transparency to their cooperation with government requests,[291] the service withdrawal dynamics following the WikiLeaks disclosures suggest a pressing need for further development of such intermediary ethics.

Returning to the descriptive point, outside of the payment context, the attempts to strangle Wikileaks have been ineffective. That conclusion, like the discussion of intermediation by publishers, suggests a need to focus heavily on the environment for leaks.

C. The Environment for Leaks

Sections III.A and III.B outlined the limits of the law as a tool to curtail secondary transmissions of leaked information through ex ante or ex post regulation of a publisher, or by reliance on nonpublisher intermediaries. These discussions highlight the need to focus more directly on the source of the leak. I begin by examining the legal environment facing a would-be leaker. After exploring the technological and other factors creating a pressure for leaks in light of that legal framework, I offer preliminary thoughts on possible reforms.

1. The Classification and Nondisclosure Regime

Understanding the environment for leaks requires some discussion of the framework for classifying government material and protecting material with classified status. Since 1940, successive presidents have, by executive order, authorized or directed government officials to classify certain materials related to the national defense. Presidential authority in this area is said to flow from

291. For example, Google's "Transparency Report" provides data on Google's cooperation with government requests to remove content and to disclose user data. *See Transparency Report*, GOOGLE, http://www.google.com/transparencyreport (last visited Jan. 18, 2012). Twitter's effort to lift a gag order on a subpoena requesting information about individuals connected to WikiLeaks provides another example. *See* Noam Cohen, *Twitter Shines a Spotlight on Secret F.B.I. Subpoenas*, N.Y. TIMES, Jan. 9, 2011, http://www.nytimes.com/2011/01/10/business/media/10link.html.

constitutional and statutory sources.[292] The current order, Executive Order 13,526, permits certain executive officials to classify information if, among other things, "the information is owned by, produced by or for, or is under the control of the United States Government" and the "classification authority determines that the unauthorized disclosure of the information *reasonably could be expected to result in damage to the national security*, which includes defense against transnational terrorism, and the original classification authority is able to identify or describe the damage."[293] Once information is classified, the government has a variety of tools to protect it. Executive Order 13,526 limits access to classified information to individuals whom the relevant agency head clears for such access, who have a need to know the information, and who sign a nondisclosure agreement.[294]

The government has successfully enforced the terms of nondisclosure agreements through injunctive relief against the employee.[295] In addition,

292. President Roosevelt's 1940 order, Exec. Order No. 8381, 3 C.F.R. 634 (1938-1943), invoked as authority the 1938 "censorship" statute, requiring the President to "define certain vital military and naval installations or equipment as requiring protection against the general dissemination of information relative thereto." Act of January 12, 1938, ch. 2, § 1, 52 Stat. 3, 3 (codified at 18 U.S.C. § 795 (2006)). Later executive orders set classification standards based not on specific statutory authority, but on "authority vested" in the President "by the Constitution and statutes of the United States." *See, e.g.*, Exec. Order No. 11,652, 3 C.F.R. 375, 375 (1973). The current executive order on classified information, Executive Order 13,526, similarly cites presidential authority created "by the Constitution and the laws of the United States of America." Exec. Order No. 13,526, 75 Fed. Reg. 707, 707 (Dec. 29, 2009).

293. Exec. Order No. 13,526, § 1.1, 75 Fed. Reg. at 707 (emphasis added). In addition, the order provides that "[i]nformation shall not be considered for classification unless its unauthorized disclosure could reasonably be expected to cause identifiable or describable damage to the national security" and it pertains to at least one of the following:

> (a) military plans, weapons systems, or operations;
> (b) foreign government information;
> (c) intelligence activities (including covert action), intelligence sources or methods, or cryptology;
> (d) foreign relations or foreign activities of the United States, including confidential sources;
> (e) scientific, technological, or economic matters relating to the national security;
> (f) United States Government programs for safeguarding nuclear materials or facilities;
> (g) vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security; or
> (h) the development, production, or use of weapons of mass destruction.

Id. § 1.4, 75 Fed. Reg. at 709.

294. *Id.* § 4.1, 75 Fed. Reg. at 720.

295. *See* United States v. Marchetti, 466 F.2d 1309, 1311 (4th Cir. 1972); *see also* Snepp v. United States, 444 U.S. 507, 509-10 (1980) (upholding a constructive trust for profits a book

various criminal statutes prohibit government employees from disclosing or mishandling certain types of classified information.[296] The Espionage Act, discussed in Part II for its potential applicability to secondary transmission of national security information, does not refer to "classified" information but prohibits the disclosure of certain information connected to or relating to the national defense.[297] As previously noted, current 18 U.S.C. § 793(d), which derives from section 1(d) of the 1917 Act, prohibits one with lawful possession of national defense information from willfully communicating, delivering, or transmitting that information "to any person not entitled to receive it."[298]

As with § 793(e), discussed in Part II, the key question is whether this prohibition criminalizes "leaks" of classified information preparatory to publication, or whether it reaches only those disclosures made in connection with what we might view as classic espionage (that is, the transmission of information to a foreign government). Subsections 793(d)-(e) were originally part of the same section of the Espionage Act, before Congress in 1950 split the section into separate provisions governing one who "lawfully" had possession of national defense information and one who had "unauthorized" possession of such information.[299] The statutory text and structure point to the conclusion that § 793(d)'s prohibition on the disclosure of certain national defense information extends beyond disclosures to a foreign government. More analysis is required before we can conclude that the Act covers "leaks" to the press, however.

The first issue is how, if at all, the First Amendment cabins interpretation of the statute. There is only one reported case in which the statute has been used to prosecute a defendant seeking to transmit information for purposes of publication. In *United States v. Morison*, a Navy employee provided classified photographs of a Soviet aircraft carrier and a summary of an explosion at a

employee failed to submit for prepublication review under the terms of a nondisclosure agreement, despite the agency's stipulation that the book did not contain confidential information); Motions Hearing Transcript at 21, United States v. Jones, Civ. No. 10-765 (E.D. Va. June 15, 2011), *available at* http://www.fas.org/sgp/jud/jones/061511-hearing.pdf (granting motion for partial summary judgment on breach of contract claim where defendant published manuscript despite adverse outcome of prepublication review process).

296. *See, e.g.*, 18 U.S.C. § 798 (prohibiting disclosure of information concerning cryptographic and communications intelligence systems); 50 U.S.C. § 783 (prohibiting U.S. government officers and employees from communicating classified information to an agent of a foreign government); *see also* 18 U.S.C. § 1924 (prohibiting knowing removal of classified information with intention of keeping that material in an unauthorized location).

297. 18 U.S.C. § 793(d)-(e).

298. *Id.* § 793(d).

299. *See supra* note 180 and accompanying text.

Soviet naval base to a British publisher.[300] In challenging his conviction under § 793(d)-(e), the defendant claimed that the Espionage Act must be read to exempt leaks to the press, otherwise the provisions would violate the First Amendment. The Fourth Circuit rejected that claim, concluding that the First Amendment does not categorically bar the prosecution of one who transmits national defense information to the press.[301] The Fourth Circuit drew upon the Supreme Court's decision in *Branzburg v. Hayes*, in which the Court rejected a reporter's claim that a grand jury subpoena requiring him to expose the identity of his informants could not be enforced without violating a First Amendment-protected privilege to gather news.[302] The *Morison* court reasoned that *Branzburg*, along with cases rejecting First Amendment objections to enforcement of confidentiality agreements signed by government employees,[303] required the conclusion that

> a recreant intelligence department employee who had abstracted from the government files secret intelligence information and had [willfully] transmitted or given it to one "not entitled to receive it" as did the defendant in this case, is not entitled to invoke the First Amendment as a shield to immunize his act of thievery.[304]

Beyond whether the First Amendment immunizes leaks intended for publication, a second issue is whether a defendant's intent in transmitting national defense information to a publisher can be consistent with the scienter

300. United States v. Morison, 844 F.2d 1057, 1060-61 (4th Cir. 1988).

301. *Id.* at 1068. The opinions in *Morison* demonstrate divergent views among the judges on the First Amendment issue. Writing for the court, Judge Russell stated that "we do not perceive any First Amendment rights to be implicated here." *Id.* Although Judge Wilkinson joined that opinion, he also wrote in his concurrence that the First Amendment interests involved in the case are not "insignificant." *Id.* at 1081 (Wilkinson, J., concurring). He concluded, rather, that "the First Amendment imposes no blanket prohibition on prosecutions for unauthorized leaks of damaging national security information." *Id.* at 1085. As for the application of the statute to the defendant, Judge Wilkinson concluded that the district court's jury instruction, which required proof that the disclosures were potentially damaging to national security, eliminated any First Amendment concern. *Id.* at 1083-84. Judge Philips agreed with Judge Wilkinson's assessment of the significance of the First Amendment interests as well as the conclusion that application of the statute to the defendant was consistent with the First Amendment. *Id.* at 1085-86 (Phillips, J., concurring specially).

302. Branzburg v. Hayes, 408 U.S. 665, 679-708 (1972).

303. *See* Snepp v. United States, 444 U.S. 507, 507-10 (1980); United States v. Marchetti, 466 F.2d 1309, 1317 (4th Cir. 1972).

304. *Morison*, 844 F.2d at 1069.

requirement that the statute (within constitutional limits) imposes. The Espionage Act contains several different intent requirements. Section 794(a)'s prohibition on transmitting information to a foreign government requires proof that the defendant had "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."[305] Similar requirements appear in § 793(a), which prohibits entering a U.S.-owned or U.S.-controlled facility for the purpose of obtaining certain defense information, and § 793(b), which prohibits gathering national defense materials. The provisions governing the communication, delivery, or transmission of national defense information, however, do not contain the same requirement. Rather, § 793(d)-(e) each require a showing that the defendant acted "willfully"—a term that courts have defined in this context as requiring proof of bad faith[306] or a specific purpose to do that which the law proscribes.[307] In addition, courts construing § 793(d) (or the parallel provision in § 793(e)) have concluded that the statute covers only information that the defendant knows or has reason to believe could be used to the injury of the United States or to the benefit of a foreign nation.[308]

This construction draws upon cases addressing claims that portions of the Espionage Act are void for vagueness under the Due Process Clause of the Fifth Amendment. In the 1941 case of *Gorin v. United States*,[309] the Supreme Court considered what qualified as "national defense" information under the Espionage Act. The case involved an investigator in a U.S. naval intelligence office who delivered certain reports to a Soviet agent.[310] The defendants were charged under sections 1(b) and 2(a) of the Espionage Act,[311] the precursors to § 793(b) on gathering national defense material and §794(a) on transmitting it to a foreign government. In challenging their convictions, the defendants claimed that the Espionage Act as a whole covered only national defense information connected with the U.S.-owned or U.S.-controlled protected places enumerated in section 1(a) of the Act (e.g., vessels, navy yards, forts,

305. 18 U.S.C. § 794(a) (2006).

306. *See* United States v. Truong Dinh Hung, 629 F.2d 908, 919 (4th Cir. 1980).

307. *See Morison*, 844 F.2d at 1073.

308. *See, e.g.*, United States v. Rosen, 445 F. Supp. 2d 602, 622 (E.D. Va. 2006) (denying pretrial motion to dismiss charges for violation of § 793(d) and conspiracy to violate § 793(e); concluding that to qualify as information relating to the national defense, the information must be of the type that "if disclosed, could threaten the national security of the United States").

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

310. *Id.* at 22.

311. *Id.* at 21.

etc.).[312] The defendants claimed that unless so construed, the statute would be unconstitutionally vague, because it would otherwise reach an indefinite range of "generally published and available" information "connected with" the national defense, such as reports on food production, advances in civil aeronautics, and so forth.[313]

In rejecting this claim, the Court observed that the words "national defense" have a "well understood connotation," referring "to the military and naval establishments and the related activities of national preparedness."[314] Despite the breadth of this category, the Court reasoned that a bad faith requirement necessarily cabined the statutory provisions.[315] Each of the provisions under which the defendants were charged required proof that the defendants intended or had reason to believe that the information to be obtained or communicated "is to be used to the injury of the United States or to the advantage of a foreign nation."[316] The bad-faith requirement removed from the statute any publicly available defense information, for, as the Court reasoned, "where there is no occasion for secrecy," there could be "no reasonable intent to give an advantage to a foreign government."[317] The Court concluded that the statute, so construed, "appears sufficiently definite to apprise the public of prohibited activities and is consonant with due process."[318]

As noted earlier, the requirement that a defendant intend or have reason to believe that national defense information will be used to injure the United States or to benefit a foreign nation appears in §§ 793(a)-(b) and 794(a).[319] Section 793(c)'s prohibition on receiving national defense information, by contrast, requires only that the defendant act with knowledge that the information has been obtained contrary to the provisions of the Espionage Act.[320] Subsections 793(d)-(e) prohibit the "willful[]" communication,

312. *Id.* at 23.

313. *Id.*

314. *Id.* at 28 (quoting Brief for the United States at 42, *Gorin*, 312 U.S. 19 (Nos. 87, 88)).

315. *Id.*

316. *See* Espionage Act of 1917, ch. 30, § 1(b), 40 Stat. 217, 218 (incorporating scienter requirement of § 1(a)); *id.* § 2(a), 40 Stat. at 218.

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

318. *Id.*

319. *See supra* text accompanying notes 305-308.

320. 18 U.S.C. § 793(c) (2006).

delivery, transmission, or retention of covered material and information.[321] In the wake of *Gorin*, one question for the courts was whether *Gorin*'s resolution of the due process challenge extended to portions of the Espionage Act that do not explicitly require that the defendant intend or have reason to believe that the relevant national defense information is to be used to the injury of the United States or to the advantage of a foreign nation. Although the Court in *Gorin* linked the secrecy requirement to the scienter requirements in the provisions at issue in that case—requirements that, as noted, now appear in §§ 793(a)-(b) and 794(a), but not in § 793(c)-(e)—lower courts have interpreted *Gorin* to restrict the Espionage Act's coverage to information that is "closely held" by the government.[322] Similarly, even for provisions with a different scienter requirement than the provisions at issue in *Gorin*, courts have held that national defense information is limited to information that, if

321. In 1950, Congress rewrote § 793(d)-(e) to prohibit not only the transmission of documents and similar tangible items, but also the transmission of "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." Subversive Activities Control Act of 1950, ch. 1024, § 18, 64 Stat. 987, 1004 (codified as amended at 18 U.S.C. § 793(d)-(e)). Subsections 793(d)-(e) thus contain a phrase similar to the ones appearing in § 793(a)-(b) and § 794(a). The question these provisions raise is whether the "relating to the national defense which information . . ." phrase modifies "information," or modifies all of the preceding items in the list. For a conclusion that it modifies only "information," so as to impose an additional scienter requirement on transmission of intangible information as opposed to documents, see *United States v. Rosen*, 445 F. Supp. 2d 602, 625-26 (E.D. Va. 2006).

322. *See, e.g.*, United States v. Squillacote, 221 F.3d 542, 576 (4th Cir. 2000) (rejecting a challenge to a conviction under § 793(b) and § 794(a) where the district court instructed the jury that the government must prove that the documents were "closely held"); United States v. Morison, 844 F.2d 1057, 1071-73 (4th Cir. 1988) (rejecting a challenge to a conviction under § 793(d)-(e) where the district court instructed the jury that the government must prove that the documents were "closely held"); United States v. Truong Dinh Hung, 629 F.2d 908, 918 n.9 (4th Cir. 1980) (upholding, in a case involving §§ 793(e) and 794(a), jury instructions stating that defendants could not be convicted based on transmission of information available in the public domain); United States v. Dedeyan, 584 F.2d 36, 39-40 (4th Cir. 1978) (in a case involving the "failure to report" provision of § 793(f)(2), upholding a jury instruction that defined "national defense" information to exclude information "made public by Congress or the Department of Defense" and "lawfully available to the general public"); United States v. Abu-Jihaad, 600 F. Supp. 2d 362, 386-87 (D. Conn. 2009) (rejecting a challenge to a conviction under § 793(d), where a jury instruction stated that information relating to the national defense must be "closely held" and cannot be publicly available); *Rosen*, 445 F. Supp. 2d at 622 (rejecting a pretrial motion to dismiss; concluding that, for purposes of § 793(d)-(e), national defense information requires "that the information be a government secret"); *see also* United States v. Heine, 151 F.2d 813, 816 (2d Cir. 1945) (overturning conviction under section 2(a) of the Espionage Act on the ground that the information was publicly available).

disclosed, would potentially injure the United States or benefit a foreign government.[323]

As this discussion suggests, the text, structure, and case law point to the conclusion that the Espionage Act reaches disclosures of information unconnected with classic espionage. Courts have construed "national defense information" to encompass only information closely held by the government that, if disclosed, could injure the United States or benefit a foreign government. Courts have concluded that, when so construed, the Espionage Act is not unconstitutionally vague. Nor does applying the statute to one who intends that the media publish the information violate the First Amendment.

Implicit in this discussion is the fact that the phrase "national defense information" used throughout §§ 793 and 794 is not coterminous with the phrase "classified information." Because the Espionage Act well predates the current classification system, that disjunction is unsurprising. Courts have observed, however, that a document's classification status can be relevant to the question of whether a document is related to the "national defense."[324] In theory, a document's classification status could provide evidence that the document was closely held or that the document, if transmitted, would injure the United States or aid a foreign nation.[325]

With this understanding of the classification system and the framework protecting against disclosure, we can explore the pressure for leaks.

2. *The Pressure for Leaks*

Apart from the legal framework, at least four other interrelated factors shape the environment for leaks: the sheer volume of defense-related information available, the problem of "overclassification" that contributes to that volume, the broad range of access to that information, and the ease of

323. *See, e.g.*, *Morison*, 844 F.2d at 1072 (rejecting a challenge to a conviction under § 793(d)-(e) where the court instructed the jury that the government must prove that the materials "would be potentially damaging to the United States or might be useful to the enemy of the United States" (quoting United States v. N.Y. Times Co., 403 U.S. 713, 740 (1971) (White, J., concurring))); *Dedeyan*, 584 F.2d at 39-40 (approving the district court's limiting instruction under § 793(f), which required the government to prove that disclosure would be "potentially damaging to the national defense, or that information in the document disclosed might be useful to an enemy of the United States"); *Rosen*, 445 F. Supp. 2d at 635 (interpreting national defense information to require a showing that the information is the type which, if disclosed, could threaten the national security of the United States).

324. *See Truong Dinh Hung*, 629 F.2d at 918 n.9; *Dedeyan*, 584 F.2d at 40.

325. *See supra* note 293 (noting that information cannot be classified unless its disclosure could reasonably be expected to harm national security).

compactly reproducing such information. Leaving the problem of overclassification aside for the moment, a comparison of the current environment for leaks to Ellsberg's leak of the Pentagon Papers study is instructive.

Ellsberg was an analyst who knew of the existence of the Pentagon Papers from his own participation in the project as a RAND Corporation employee. Only a small number of analysts and officials knew the study existed, and access to it was tightly controlled.[326] In contrast, the post-September 11 imperative for better information-sharing has required a substantial increase in the number of employees who have access to classified information. The system from which Bradley Manning allegedly extracted classified information was accessible not to a handful of high-level employees, but to hundreds of thousands of government employees across the Department of Defense.[327] In light of the existence of inexpensive high-volume storage media, the government can collect (or produce) and retain much more information in digital form than it could have in hard copy. The publishers that worked with the WikiLeaks documents estimated that the databases were 120 times the size of the forty-seven-volume Pentagon Papers study.[328] For Ellsberg, reproducing the Pentagon Papers study was tedious. Ellsberg apparently smuggled the study out of a safe chapter by chapter for late-night photocopying sessions at the office of a coworker's friend.[329] Private Manning, in contrast, allegedly used high-volume compact storage to reproduce an extraordinary amount of information undetected.[330]

In addition to the access and technological considerations that increase the volume of information available to a would-be leaker, we must consider how the problem of overclassification contributes to that volume of information. Overclassification is not a new phenomenon. The *Pentagon Papers* case itself provides a near-comical example. One volume of the study contained only the

326. ELLSBERG, *supra* note 27, at 232-34.

327. *Information Sharing in the Era of WikiLeaks: Balancing Security and Collaboration: Hearing Before the S. Comm. on Homeland Sec. and Governmental Affairs*, 112th Cong. 2 (2011) (joint testimony of Teresa Takai, Chief Info. Officer and Acting Ass't Sec'y of Defense for Networks and Info. Integration, and Thomas Ferguson, Principal Deputy Under Sec'y of Defense for Intelligence) (noting that there are between 400,000 and 500,000 Department of Defense users of SIPRNet).

328. *See* Rusbridger, *supra* note 238, at 5 (estimating that the WikiLeaks materials contained 300 million words, as compared with 2.5 million words in the Pentagon Papers study).

329. ELLSBERG, *supra* note 27, at 299-305; SCHRAG, *supra* note 27, at 46-47.

330. *See* Hansen, *supra* note 140.

public statements of former Presidents Kennedy and Johnson.[331] Because a compilation must carry the highest classification level of the documents it contains, such public statements were deemed "top secret." High-level government officials discussing the problem of overclassification have suggested that between 50% and 90% of national security information is improperly classified.[332] Part of the problem is structural. The current classification system tilts toward overclassification: lower-level bureaucrats risk less by erring on the side of classification, and their superiors are unlikely to dislodge these decisions. In light of the slow pace of declassification—ironically, the declassification of the full Pentagon Papers study coincided with the forty-year anniversary of the original unauthorized leak[333]—officials are not held accountable for erroneous classification decisions.

How do these factors—the sheer volume of information, the problem of overclassification, the breadth of access to information, the ease of reproduction—affect the way we think about leaks of classified information? These factors may make leaks more likely. The breadth of access, volume of information available, and ease of reproduction mean that there are more points at which leaks can occur. Moreover, the dramatic differences between the legal environment for unauthorized leaks and the legal environment for downstream disclosure of such leaks may contribute to the pressure for leaks. Ex ante, the legal framework appears to permit equitable relief against a would-be leaker's disclosure of classified information based on the employee's contractual relationship with the government, even without a case-by-case evaluation of the value of the disclosure or the danger to national security. By contrast, the government cannot enjoin the downstream publisher from disclosing classified information except in the rarest of circumstances. Ex post, the government can punish the leaker, but punishment of the downstream publisher is much more uncertain.[334] If a would-be leaker correctly perceives that the downstream publisher's potential for liability is unlikely to constrain the decision to publish, the leaker may be more willing to disclose information than he or she would be if the publisher needed to weigh the risks more carefully.

331. RUDENSTINE, *supra* note 3, at 205.

332. *See, e.g.*, Constitutional Issues Hearing, *supra* note 168 (statement of Thomas Blanton, Director, National Security Archive, George Washington University).

333. *See Pentagon Papers*, NAT'L ARCHIVES, *available at* http://www.archives.gov/research/pentagon-papers (last visited Sept. 15, 2011).

334. *See supra* notes 221-236 and accompanying text.

3. Shaping the Environment for Leaks

This discussion of the pressure for leaks suggests a number of possible responses. One is simply to recognize the value that some unauthorized leaks have for public discourse and to take a minimalist approach. As Parts I and II suggested, however, the case thought to provide the normative framework for this approach—the *Pentagon Papers* case—does not. While forms of First Amendment absolutism may provide an alternative normative framework supporting this approach, that framework does not suitably address situations involving the potential for significant harm, other than to assume that relocating the assessment of harm close to the source and away from traditional intermediaries is unproblematic.

It is obvious that any strategy for shaping the environment for leaks must focus on the technical as well as the legal environment. Regarding the structure of the government information systems affected by the disclosures, one could argue that notwithstanding the post-September 11 imperative for better information-sharing, the fact that an individual at Private Manning's rank had access to the range of information the disclosures revealed demonstrates deeply flawed government information security practices. The principle of "least privilege," for example, requires that each user have access only to the information necessary for the user to perform his or her assigned functions.[335] The agencies affected by the WikiLeaks disclosures appear to have taken a number of steps to improve their information security practices, including requiring multiple users to authenticate the copying of classified data and segregating certain data from networked systems.[336] The WikiLeaks disclosures also emphasize the need for tools to detect anomalous data activity from sources inside as well as outside of the affected network and the possible need for insider threat profiling. There is little we can gather about the government's detection tools other than that they failed in this instance, and it is therefore difficult to recommend concrete steps for improvement.

I focus here on the possible legal responses to the shifts the WikiLeaks disclosures reveal. It is important to acknowledge, however, the complex connection between the technical environment and the legal environment: reshaping the legal environment for leaks may reduce the government's

335. *See, e.g.*, Cem Paya, *Quasi-Secrets: The Nature of Financial Information and Its Implications for Data Security*, *in* HARBORING DATA: INFORMATION SECURITY, LAW, AND THE CORPORATION 121, 127 (Andrea M. Matwyshyn ed., 2009).

336. *See generally Security Clearances: Hearing Before the Intelligence Cmty. Mgmt. Subcomm. of the H. (Select) Intelligence Comm.*, 112th Cong. (2010) (discussing security clearance reform and information access across defense agencies).

incentives to reshape the technical environment through better information security practices.

a. The Espionage Act

The first potential reform involves reassessing how the law should deter and respond to leaks. As discussed above, even though § 793(d) may well reach leaks, the statute has not been significantly amended since 1950. There are at least three key issues a statute addressing unauthorized leaks must face.

The first is the coverage of the statute. Because the Espionage Act predates the classification system, the category of covered information is ill-defined. Courts have understood the statute to cover closely held information concerning the national defense or military preparedness, which information may cause injury to the United States or benefit a foreign government.[337] Narrowing the coverage of an antileak statute to classified information would address lingering concerns about vagueness.

The second and more critical issue concerns the statute's scienter requirement. Unlike several other portions of the Espionage Act, § 793(d) does not by its terms require a showing that the defendant had an intent or reason to believe that disclosure would harm the United States or benefit a foreign government.[338] Courts have construed the statute to require knowledge or reckless disregard of the possibility that disclosure of the underlying material would injure the United States or benefit a foreign government. Even when the court-imposed definition of national defense information is read alongside the statutory requirement of willfulness, § 793(d) appears to create broader liability than provisions such as §§ 793(a)-(b) and 794(a). There are a number of ways to resolve this issue. First, even if the provision, as interpreted by the courts, strikes an appropriate balance between criminalizing and protecting unauthorized leaks, there is a strong argument that the scienter requirement should be explicit rather than based on a strained interpretation of the

337. Gorin v. United States, 312 U.S. 19, 28 (1941); *see supra* notes 315-318 and accompanying text.

338. Subsections 793(d)-(e) each do contain an explicit requirement that the defendant know or have reason to believe that information being disclosed will harm the United States or benefit a foreign government. That language, however, appears immediately after the phrase "information relating to the national defense." At least one court has concluded that the explicit intent requirement modifies only "information relating to the national defense." *See supra* note 321. If that reading is correct, then as to the tangible items covered in § 793(d)-(e), the requirement that the defendant know or have reason to know that disclosure will harm the United States or benefit a foreign government is a judicially imposed requirement rather than an explicit statutory requirement. *See id.*

statutory text. Second, Congress could distinguish between disclosures undertaken with intent to harm the United States or benefit a foreign nation, disclosures undertaken with reckless disregard for this risk, and disclosures undertaken in bad faith and where the leaker knew or had reason to know that disclosure would pose significant national security risks. Under such a statute, disclosures undertaken with intent to harm the United States or benefit a foreign nation or disclosures undertaken with reckless disregard for such risks would warrant more substantial punishment. Third, Congress could simply limit criminal liability to cases in which a leaker intends to harm the United States or benefit a foreign nation or acts in reckless disregard of that risk.

Even the first approach—essentially a codification of judicial interpretation of the statute—would be preferable to the status quo, because it would provide greater certainty about the scope of the statute. The second approach's differentiation among categories of defendants is preferable to the first approach. The difficult question is whether the third approach, when considered alongside other statutory and contractual constraints on disclosure, is a sufficient deterrent and response to the employee whose malicious intent will be difficult to establish, or to the benignly motivated employee whose assessment of the relative benefits and harms of disclosure is simply misguided. Neither the First Amendment nor the Due Process Clause appears to require limiting liability to the cases envisioned under the third approach.[339] As I discuss below, moreover, if the second approach were linked to expanded pathways for intra-agency, intra-executive, or intragovernmental disclosures of wrongful governmental conduct, then one of the justifications for narrower criminal liability for unauthorized leaks—that of bringing to light government misdeeds—would have less force.

The third issue concerns whether the statute should be amended to permit a defendant to raise improper classification as an affirmative defense to prosecution under § 793(d). A number of defendants have raised such a defense, but courts have not accepted it. As discussed below, if improper classification remains a major problem, an unauthorized leak may serve the function of "correcting" an erroneous classification decision. Such a defense should perhaps be available only if a would-be leaker first attempts to correct improper classification through intra-agency or intragovernmental channels.

339. *See supra* notes 300-313.

b. Overclassification

In addition to addressing disclosure of leaked information directly, Congress and the executive must address the problem of overclassification. While not all unauthorized leaks are responses to overclassification, both the *Pentagon Papers* case and the WikiLeaks disclosures provide evidence of the phenomenon. The WikiLeaks disclosures effectively represented a rapid, wholesale "declassification" of massive amounts of classified material, including some information that was properly classified and other information that was not. One can sympathize with the claim that some of the material ought not to have been classified while still having discomfort with this process of "declassification" as well as the elimination of deference to the executive's judgment that disclosure would potentially cause harm.

This problem calls both for efforts to address overclassification directly—an explicit but as yet unmet goal of the Obama Aministration—and for efforts to provide alternative channels for insiders to bring forward classified evidence of governmental misconduct. In theory, whistleblower statutes protect government employees from retaliation for disclosing government misconduct. One significant statute, the Civil Service Reform Act of 1978,[340] prohibits certain adverse personnel actions against a government employee who discloses unlawful conduct. More specifically, the statute provides two protected options for disclosure that an employee "reasonably believes" evidences, among other things, "a violation of any law, rule, or regulation," an "abuse of authority," or a "substantial and specific danger to public health or safety."[341] First, if the disclosure "is not specifically prohibited by law and if such information is not specifically required by Executive Order to be kept secret in the interest of national defense or the conduct of foreign affairs,"[342] the Act does not restrict the prospective recipient of the information. Second, a disclosure may be made "to the Special Counsel [of the Merit Systems Protection Board], or to the Inspector General of an agency or another employee designated by the head of the agency to receive such disclosure."[343] This provision of the statute does not exclude disclosures that are otherwise prohibited by law or that concern information that is classified, thus permitting intra-executive disclosure of classified evidence of misconduct.

340. Civil Service Reform Act of 1978, Pub. L. No. 95-454, 92 Stat. 1111 (codified as amended in scattered sections of 5 U.S.C.).

341. 5 U.S.C. § 2302(b)(8)(A) (2006).

342. *Id.*

343. *Id.* § 2302(b)(8)(B).

Despite the fact that these provisions provide some avenues for disclosure of classified information that may reveal unlawful acts, the statute excludes several categories of employees. First, the statute does not cover members of the military. A separate federal statute, the Military Whistleblowers Protection Act, prohibits retaliatory personnel actions against members of the armed forces who report unlawful conduct, an abuse of authority, or a danger to the public health or safety, if the report is made to a Member of Congress, the Inspector General for the Department of Defense, or certain other designated persons.[344] Second, the statute excludes a number of agencies from its protection, including the Federal Bureau of Investigation, the Central Intelligence Agency, the Defense Intelligence Agency, the National Security Agency, and, "as determined by the President, any executive agency or unit thereof the principal function of which is the conduct of foreign intelligence or counterintelligence activities."[345] A separate portion of the statute covers employees of the Federal Bureau of Investigation.[346] For other employees falling within this intelligence exception, the provisions of the more recently enacted Intelligence Community Whistleblower Protection Act of 1998 may apply.[347] That statute protects intelligence community whistleblowers who follow detailed procedures for disclosing matters of "urgent concern," a category that includes evidence of flagrant lawbreaking and lying to Congress. The employee must first report the matter to the relevant agency's Inspector General, provide notice to the head of the organization, and receive direction concerning how the information can be communicated in a manner consistent with appropriate security practices.[348] An employee who follows these

344. 10 U.S.C. § 1034. Although as some have observed, the Military Whistleblowers Protection Act does not fully protect communications that are "unlawful," *see, e.g.*, Mary-Rose Papandrea, *Lapdogs, Watchdogs, and Scapegoats: The Press and National Security Information*, 83 IND. L.J. 233, 247 (2008), the Act still does provide an avenue for disclosure of classified information in connection with unlawful, abusive, or dangerous activity. The Act prohibits reprisals based on (1) communications to Members of Congress or an Inspector General that cannot be restricted—that is, communications that are not unlawful; or (2) communications to Members of Congress, an Inspector General, or certain other designated officials, when the communications disclose information the individual reasonably believes to constitute evidence of, for example, unlawful, abusive, or dangerous conduct. The latter category is not restricted based on whether the communication itself is unlawful (by virtue of disclosing classified information, for example).

345. 5 U.S.C. § 2302(a)(2)(C)(ii).

346. *Id.* § 2303.

347. Pub. L. No. 105-272, §§ 702-703, 112 Stat. 2396, 2414-17.

348. 5 U.S.C. app. 3 § 8H(d)(1)-(2).

procedures is protected from reprisals if he or she reports the relevant information to one of the congressional intelligence committees.

Aspects of these statutes remain highly controversial, for critics charge that they provide illusory protection for government employees who seek to disclose unlawful government practices.[349] Those criticisms extend across the board, with respect to unclassified as well as classified information. In the case of the WikiLeaks disclosures, some observers simply view Bradley Manning as a "whistleblower" whose actions federal law ought to protect. If the material Manning revealed indeed supplied evidence of abuse of authority or unlawful conduct, then the terms of existing law likely could have protected the disclosures through appropriate pathways, by its terms though perhaps not in practice. Because revealing classified information to the media rather than via an intra-agency or intragovernment pathway opens the material for widespread disclosure, it is especially important to clarify the pathways for confidential disclosure of classified information revealing government misconduct.

CONCLUSION

The *Pentagon Papers* case is a powerful weapon for defenders of WikiLeaks. The Supreme Court cleared a path for the *New York Times*, the *Washington Post*, and other publishers to lay the study before the American public, and history vindicated the publishers' actions. The lessons of the case for the WikiLeaks disclosures, however, are more complicated than they first appear. The *Pentagon Papers* case did not presume a shared conception of the public interest and of harm between the source of a leak and the potential publisher. Rather, the separate opinions in the case illustrate a key assumption shared by a majority of the Justices: that the possibility of criminal liability, and an ethical responsibility to prevent harm, would shape how the publishers used the Pentagon Papers.

These constraints on downstream disclosure may well be illusory. Recognizing that fact highlights a different set of lessons from the *Pentagon Papers* case than WikiLeaks' defenders would draw, requiring not that we celebrate the unauthorized leaks but that we address the asymmetries and gaps that led to them.

349. *See, e.g.*, *Whistleblower Protection Enhancement Act of 2009: Hearing Before the Subcomm. on Oversight of Gov't Mgmt., the Fed. Workforce, & the Dist. of Columbia of the S. Comm. on Homeland Sec. and Govt'l Affairs*, 111th Cong. 57-97 (2009) (testimony of Thomas Devine, Legal Director, Gov't Accountability Project).