CONSIDER THE CENSOR

DEREK E. BAMBAUER †

I. UNCERTAINTY'S VIRTUES

Nixon could have won.

This is the key lesson from the *Pentagon Papers* case, as the recent controversy surrounding WikiLeaks demonstrates. The fight between Daniel Ellsberg, the *New York Times*, and the administration of President Richard Nixon is typically celebrated as a triumph for free speech and for transparency in government.[1] The Supreme Court's 6–3 decision confirmed the ability of the *Times* and the *Washington Post* to engage in whistle-blowing by publishing sensitive government documents during wartime.[2] The Nixon administration claimed that the purloined papers would compromise national security.[3] In fact, the documents showed that a succession of American administrations had mis-portrayed the war, which was going far more poorly than popularly believed. The level of damage to national security from the Papers' publication is unknown, but widely be-

---

† Associate Professor of Law, Brooklyn Law School. Thanks for helpful suggestions and discussion are owed to Dan Hunter, Thinh Nguyen, and Jane Yakowitz. The author welcomes comments at derek.bambauer@brooklaw.edu.

1. *See, e.g.*, David A. Strauss, *Freedom of Speech and the Common-Law Constitution*, *in* ETERNALLY VIGILANT: FREE SPEECH IN THE MODERN ERA 33, 58–59 (Lee C. Bollinger & Geoffrey R. Stone eds., 2003).

2. New York Times Co. v. United States (*Pentagon Papers*), 403 U.S. 713 (1971) (per curiam).

3. *E.g.*, Brief for the United States (Secret Portion), *Pentagon Papers*, 403 U.S. 713 (1971) (Nos. 1873, 1885) (listing secret information contained in the Pentagon Papers that Solicitor General Erwin Griswold argued would be highly damaging to U.S. national security).

lieved to be low.[4] Thus, the standard narrative is celebratory: the First Amendment and a vigilant, dogged press defeated the government's self-serving efforts to conceal the slow failure of the Vietnam War.

The current controversy over WikiLeaks calls this straightforward victory narrative into question.[5] The WikiLeaks website is a whistleblower's dream, offering secure, anonymous access to those who want to share information.[6] WikiLeaks overtly claims the mantle of the Pentagon Papers as its own.[7] The site sprang into prominence in April 2010 when it made available gun camera footage from a U.S. Army attack helicopter operating in Baghdad in 2007;[8] the footage showed an attack on people who, it was later discovered, included two Reuters employees.[9] WikiLeaks went from fame to notoriety in November 2010 when it began publishing thousands of diplomatic cables from the U.S. Department of State along with internal documents from the Department of Defense about the conflicts in Iraq and Afghanistan.[10] The site became a focus of criticism from across the American political spectrum,[11] with some

---

4. *See* DAVID RUDENSTINE, THE DAY THE PRESSES STOPPED 3–5 (1998) (reviewing the possible damage from publication of the Papers and concluding that such damage was lower than widely believed).

5. *See, e.g.*, William H. Freivogel, *Analysis: Are WikiLeaks the 21st Century's Pentagon Papers?*, ST. LOUIS BEACON, Dec. 7, 2010, http://www.stlbeacon.org/issues-politics/nation/106722-comparison-of-wikileaks-with-pentagon-papers (comparing the *Pentagon Papers* case and the WikiLeaks controversy and in both cases observing complications from publishing information that was potentially harmful to national security).

6. *Submissions*, WIKILEAKS, http://wikileaks.ch/Submissions.html (last visited Mar. 19, 2011).

7. Ellen Nakashima & Joby Warrick, *Wikileaks Takes New Approach in Latest Release of Documents*, WASH. POST, July 26, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/07/25/AR2010072503356.html.

8. *WikiLeaks Posts Video of "US Military Killings" in Iraq*, BBC NEWS, Apr. 6, 2010, http://news.bbc.co.uk/2/hi/americas/8603938.stm.

9. *Leaked U.S. Video Shows Deaths of Reuters' Iraqi Staffers*, REUTERS, Apr. 5, 2010, *available at* http://www.reuters.com/article/2010/04/06/us-iraq-usa-journalists-idUSTRE6344FW20100406.

10. *See, e.g.*, 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 (discussing broad criticism of leaked cables as reckless and dangerous).

11. *See, e.g.*, Paul Owen, Richard Adams & Ewen MacAskill, *WikiLeaks: US Senator Joseph Lieberman Suggests New York Times Could Be Investigated*, GUARDIAN (LONDON), Dec. 7, 2010, http://www.guardian.co.uk/world/2010/dec/07/wikileaks-joe-lieberman-new-york-times-investigated; Justin Elliott, *Palin: Hunt Down Assange Like a Terrorist*, SALON.COM, Nov. 29, 2010, http://www.salon.com/news/politics/war_room/2010/11/29/palin_hunt_down_assange.

commentators going so far as to call for the assassination of WikiLeaks founder and Editor-in-Chief Julian Assange.[12] Although now exploring the possibility of criminal charges against Assange and other WikiLeaks collaborators,[13] the U.S. government to date has limited its efforts to suasive means, such as placing pressure on service providers to drop WikiLeaks.[14] Despite the lamentations of public figures such as Sarah Palin,[15] the United States did not attempt to enjoin the release of the documents by WikiLeaks, nor has it attempted to employ technical means to interdict ongoing releases. America's government, it seems, has learned the popular lesson of the *Pentagon Papers*: it is wrong, if not fruitless, to seek to censor information. And WikiLeaks is seen as the controversy's progeny; even *New York Times* executive editor Bill Keller asked of the site, "[W]as it different in kind from the Pentagon Papers . . . ? I think probably not."[16]

This conception of WikiLeaks is wrong, and dangerous. The positive perception of the outcome of the Pentagon Papers clash rests on two key aspects of the case that are both underappreciated and vital. First, the U.S. court system had the power to resolve the controversy—both jurisdictionally and, critically, as a matter of enforcement. If the Supreme Court had ruled against the *New York Times*, the paper would not have published further excerpts from the documents, and the information contained therein would have been disclosed only partially and later in time.[17] The outcome of the case was in doubt not merely as a matter of First Amendment doctrine, but as one of practical import: the Court's judgment would not be a

---

12. Jeffrey T. Kuhner, Op-Ed., *Kuhner: Assassinate Assange?*, WASH. TIMES, Dec. 2, 2010, http://www.washingtontimes.com/news/2010/dec/2/assassinate-assange.

13. *See, e.g.*, Ravi Somaiya & Alan Cowell, *WikiLeaks Founder Said to Fear 'Illegal Rendition' to U.S.*, N.Y. TIMES, Jan. 11, 2011, http://www.nytimes.com/2011/01/12/world/europe/12assange.html (noting that Justice Department officials are determining whether charges can be brought against Assange).

14. *E.g.*, Lance Whitney, *Amazon Cuts Off WikiLeaks*, CNET NEWS, Dec. 2, 2010, http://news.cnet.com/8301-13578_3-20024376-38.html (discussing Amazon.com's removal of WikiLeaks from its cloud computing service one day after Senator Lieberman criticized the company for hosting the site).

15. Chris Good, *Palin: We Should Have Hacked WikiLeaks*, ATLANTIC, Nov. 30, 2010, http://www.theatlantic.com/politics/archive/2010/11/palin-we-should-have-hacked-wikileaks/67200.

16. David Carr, *WikiLeaks Taps Power of the Press*, N.Y. TIMES, Dec. 13, 2010, at B1, *available at* http://www.nytimes.com/2010/12/13/business/media/13carr.html.

17. R.W. Apple, *Lessons From the Pentagon Papers*, N.Y. TIMES, Jun. 23, 1996, http://www.nytimes.com/books/97/04/13/reviews/papers-lessons.html.

dead letter.[18] (This was true in both directions: the Nixon administration would not have ignored the Court's ruling by seizing the *Times*' printing presses, for example, or imprisoning its staff.) Second, the *Times* itself played a key role as an information intermediary in maximizing the Papers' value to readers while minimizing harm.[19] 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.[20] Thus, Americans could rely on the *Times* to edit and redact the Papers, removing information of dubious public value but considerable national security danger. Victory for the paper in court resulted not in total disclosure of the underlying data, but in judicial deference to the editors' judgments about the appropriate balance between informing the public and protecting national security interests. Dissemination of the Papers was thus limited in two important respects: first, by the informed judgment of the *Times*' and *Post*'s editors, and second, by review through a judicial system with the power to enforce its conclusions.

II. WHERE WIKILEAKS FAILS

The revelation of the Pentagon Papers was legitimated by two important checks on disclosure: editorial judgment based on journalistic ethics, and the independent review of a neutral arbiter bound by process and anchored in democratic government. WikiLeaks lacks both of these protective functions. First, Internet-based information technology increasingly confers an effective code-based veto on the power of national sovereigns, such as the United States, to enforce legal writ.[21] Information repositories, such as WikiLeaks, can locate

---

18. *See* Freivogel, *supra* note 5.

19. *See, e.g.*, Arthur S. Brisbane, Op-Ed., *Sharing Secrets at Arm's Length*, N.Y. TIMES, Oct. 31, 2010, at WK8, *available at* http://www.nytimes.com/2010/10/31/opinion/31pubed.html (from the *Times*' ombudsman, comparing the *New York Times*' decision to publish leaked cables from WikiLeaks with the decision to publish the Pentagon Papers in 1971, reviewing the *Times*' decision making in the WikiLeaks case, and contending that the decision to "filter" what was published while redacting names was ethical).

20. *See, e.g.*, Daniel E. Koshland, Jr., *The Handling of Leaked Information*, 253 SCIENCE 9, 9 (1991) (setting out journalistic standards to be followed when publishing leaked information, including supplying missing information from the leaked document to provide a balanced account for readers).

21. *See generally* LAWRENCE LESSIG, CODE: VERSION 2.0 200–75 (2006) (explaining how code is regulated in cyberspace and discussing its relationship to privacy and free speech).

in countries where laws are friendly to them, while reaching consumers in countries whose laws are not.[22] Internet technology lowers the cost of information—of its acquisition, storage, indexing, and distribution—to nearly zero.[23] The Internet's ability to cross national borders seamlessly and at a low cost concomitantly reduces the traditional power of nation-states to limit information distribution.[24] These shifts change the calculus of whistle-blowing disclosure significantly. They empower those who would reveal information while undercutting those who seek to control it.

WikiLeaks has thus proved considerably immune to legal efforts to interdict its operations. In 2008, the site was sued by the Switzerland-based Bank Julius Baer ("BJB");[25] WikiLeaks had published documents that, according to a former Bank executive, demonstrated BJB's complicity in tax evasion by its clients.[26]

A U.S. federal district court judge issued an injunction to Dynadot, WikiLeaks' domain name host, which prevented the company from resolving requests for the site's wikileaks.org domain.[27] While free speech organizations rushed to the site's defense, its ability to make the purloined documents available continued unabated.

---

22. *See Swedish Law Gives Shelter to Controversial Wikileaks Site*, EURACTIV (Apr. 9, 2010), http://www.euractiv.com/en/infosociety/sweden-gives-legal-shelter-controversial-wikileaks-site-news-426138.

23. *See generally* Derek E. Bambauer, *Conundrum*, 96 MINN. L. REV. __ (forthcoming 2012) (describing cybersecurity challenges of falling information costs, such as distributed denial-of-service attacks and rapid dissemination of data after breaches).

24. *See* David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1367 (1996) (stating that international computer-based communications threaten territory-based law enforcement); Jack Goldsmith, *Seven Thoughts on Wikileaks*, LAWFARE (Dec. 10, 2010), http://www.lawfareblog.com/2010/12/seven-thoughts-on-wikileaks (explaining that countries can exercise control over the Internet within their territory but cannot exercise control internationally).

25. *See* Bank Julius Baer & Co. Ltd. v. WikiLeaks, No. 3:2008cv00824 (N.D. Cal. 2008), *available at*, http://dockets.justia.com/docket/california/candce/3:2008cv00824/200125 (last visited Apr. 11, 2011).

26. Thomas Claburn, *Swiss Banks Abandons Lawsuit Against Wikileaks*, INFORMATIONWEEK, Mar. 6, 2008, http://www.informationweek.com/news/security/privacy/showArticle.jhtml?articleID=206902154.

27. Order Granting Permanent Injunction, Bank Julius Baer & Co. Ltd. v. WikiLeaks, No. CV08-0824 (N.D. Cal. 2008), *available at* http://docs.justia.com/cases/federal/district-courts/california/candce/3:2008cv00824/200125/48 (banning Dynadot from translating requests for the wikileaks.org domain name to the relevant IP address). This prevented users who entered wikileaks.org into their browser's address bar from reaching the WikiLeaks site, but did not affect those who sought WikiLeaks at different domain names, or via the site's underlying IP address. Claburn, *supra* note 26.

WikiLeaks simply moved to new domain names, which were rapidly indexed by search engines and made available to curious Internet users.[28] Admitting defeat, the judge dissolved the injunction two weeks after instituting it.[29]

The Internet has dramatically reduced the cost of providing and accessing information. These decreased costs benefit those who disseminate information; they can evade legal regulation by locating beyond the reach of hostile judicial regimes without forgoing the ability to reach their consumers. However, this shift undercuts helpful legal prohibitions along with harmful ones.[30]

Thus far, states have not demonstrated any greater power to enforce their proscriptions through software code than they have through legal code. Neither a massive denial-of-service attack[31] (allegedly launched by a hacker sympathetic to the U.S. government[32]), nor the withdrawal of hosting,[33] payment,[34] and DNS[35] services by U.S.-based providers prevented WikiLeaks from releasing the American diplomatic cables in November 2010. Even authoritarian

---

28. Claburn, *supra* note 26.

29. Order Denying Motion for Preliminary Injunction; Dissolving Permanent Injunction; and Setting Briefing and Hearing Schedule, Bank Julius Baer & Co. Ltd. v. WikiLeaks, 535 F. Supp. 2d 980, 982 (N.D. Cal. 2008).

30. *See, e.g.*, *Child Pornography*, U.S. DEP'T OF JUSTICE, http://www.justice.gov/criminal/ceos/childporn.html (last updated Nov. 6, 2007) (noting that in the "mid-1980's, the trafficking of child pornography within the United States had been almost completely eradicated through a series of successful campaigns waged by law enforcement," but now "child pornography is readily available through virtually every Internet technology . . . .").

31. Gregg Keizer, *DoS Attacks Hammer WikiLeaks for Second Day Running*, COMPUTERWORLD, Nov. 30, 2010, http://www.computerworld.com/s/article/9198679/DoS_attacks_hammer_WikiLeaks_for_second_day_running.

32. Richard Allen Greene & Nicola Hughes, *"Hacktivist for Good" Claims WikiLeaks Takedown*, CNN.COM (Nov. 29, 2010), http://www.cnn.com/2010/US/11/29/wikileaks.hacker/index.html.

33. *See* Geoffrey A. Fowler, *Amazon Says WikiLeaks Violated Terms of Service*, WALL ST. J., Dec. 3, 2010, http://online.wsj.com/article/SB10001424052748703377504575651321402763304.html.

34. *See* Alexia Tsotsis, *PayPal VP on Blocking WikiLeaks: State Department Said It Was Illegal*, TECHCRUNCH (Dec. 8, 2010), http://techcrunch.com/2010/12/08/paypal-wikileaks; Declan McCullagh, *MasterCard Pulls Plug on WikiLeaks Payments*, CNET.COM (Dec. 6, 2010), http://news.cnet.com/8301-31921_3-20024776-281.html.

35. *See* Charles Arthur & Josh Halliday, *WikiLeaks Fights to Stay Online After U.S. Company Withdraws Domain Name*, GUARDIAN (LONDON), Dec. 3, 2010, http://www.guardian.co.uk/media/blog/2010/dec/03/wikileaks-knocked-off-net-dns-everydns. Even without a domain name, the WikiLeaks site could be located by using a search engine, such as Google, which would index the site, and direct users to it via the site's Internet Protocol (IP) address.

regimes have been unable to tame the Net's power completely.[36] While countries such as China, Iran, and Burma have imposed filtering mechanisms that limit most citizens' access to proscribed material, these states are concededly satisfied with partial success. They do not need to prevent all access to contraband material, but instead need only ensure that whatever imperfect access occurs is not a threat to their governments' interests.[37] It is still possible to access information about the Tiananmen Square massacre or the banned Falun Gong movement from within China, although it requires extra effort.[38] States can, at best, increase the cost of information access. With WikiLeaks though, even sparse or intermittent access may cause damage to U.S. interests, due to ease of redistribution and the power of interested parties—such as other nation-states, or insurgent groups—to overcome barriers and gain access.[39] In a world of nearly costless data distribution (think retweeting on Twitter) even highly limited initial access to information can rapidly blossom into ubiquity.

The Obama administration seemed to learn from the Nixon administration's experience and grudgingly accepted the WikiLeaks release.[40] However, there is one critical difference: the government

---

36. *E.g.*, Jonathan Zittrain & John Palfrey, *Internet Filtering: The Politics and Mechanics of Control*, *in* ACCESS DENIED: THE PRACTICE AND POLICY OF GLOBAL INTERNET FILTERING 29, 31–32 (Ronald J. Deibert, John G. Palfrey, Rafal Rohozinski & Jonathan Zittrain eds., 2008) (citing Saudi Arabia as a regime unable to assert complete control over the Internet content available to its citizens, but that nonetheless employs effective censorship).

37. *Id.* at 32.

38. *See* Erica Naone, *Censorship Circumvention Tools Aren't Widely Used*, TECH. REV. (Oct. 18, 2010), http://www.technologyreview.com/web/26574 (stating that while tech humanitarians have produced tools that "can be used to access the Internet freely from anywhere, fighting the restrictions placed by the governments of such countries as China and Iran," people still chose to use proxies, which do not protect the user's identity). *See generally* Nart Villeneuve, *Technical Ways to Get Round Censorship*, *in* REPORTERS WITHOUT BORDERS, HANDBOOK FOR BLOGGERS AND CYBER-DISSIDENTS 63 (Reporters Without Borders ed., 2005), *available at* http://www.rsf.org/IMG/pdf/handbook_bloggers_cyberdissidents-GB.pdf (describing and explaining Web-based circumventors, proxy servers, and other technical methods to circumvent the censorship of particular material).

39. *See, e.g.*, Siobhan Gorman, August Cole & Yochi Dreazen, *Computer Spies Breach Fighter-Jet Project*, WALL ST. J., Apr. 21, 2009, at A1, *available at* http://online.wsj.com/article/SB124027491029837401.html (describing espionage that accessed critical design data on the U.S. Joint Strike Fighter).

40. *See, e.g.*, Press Release, White House Press Secretary, Statement by the Press Secretary Concerning WikiLeaks Release (Nov. 28, 2010), http://www.whitehouse.gov/the-press-office/2010/11/28/statement-press-secretary ("We anticipate the release of what are

did not seek to enjoin WikiLeaks from publication because doing so would have been fruitless. It ill-behooves a powerful state to publicly attempt the impossible. WikiLeaks is designed to exist beyond the reach of any single government, even one as potent as the American government.[41] The United States might have been able to employ cyber warfare techniques to interdict WikiLeaks, or to drive it offline, but doing so might well have caused even greater harm by revealing American capabilities to adversaries, such as China.[42] Thus, the first key condition to classifying the *Pentagon Papers* case as a victory is lacking. There is no impartial magistrate with the power to resolve a dispute between the American government and WikiLeaks. On the Internet, jurisdiction collapses into enforcement.[43] Instead of a court of law, a handful of cyber activists held—and hold—the unilateral ability to determine what information is released, and to whom.

Second, while WikiLeaks tries strenuously to position its activities as journalism,[44] the site and its operators lack the ethical foundation that more mainstream journalists, such as reporters at the

---

claimed to be several hundred thousand classified State department cables on Sunday night that detail private diplomatic discussions with foreign governments. . . . To be clear—such disclosures put at risk our diplomats, intelligence professionals, and people around the world who come to the United States for assistance in promoting democracy and open government.").

41. In Jonathan Zittrain's classification model for governance, WikiLeaks falls into the bottom right quadrant, which is defined by a tendency towards polyarchy (choice) over hierarchy, and bottom-up rules over top-down ones. Jonathan Zittrain, *The Fourth Quadrant*, 78 FORDHAM L. REV. 2767, 2767–70 (2010). Zittrain's model has two axes, one that runs from hierarchy at one extreme to polyarchy at the other, and one that runs from top-down governance to bottom-up governance. *Id.* at 2768. This produces four zones, which Zittrain illustrates via political science examples: authoritarianism (hierarchy, top-down), anarchy (polyarchy, bottom-up), communitarianism (hierarchy, bottom-up), and corporatism (polyarchy, top-down). *Id.* at 2768–70.

42. *Cf.* RICHARD A. CLARKE & ROBERT A. KNAKE, CYBER WAR 57–61 (2010) (discussing the prospect of war with China and U.S. vulnerability to cyberattack); Seymour M. Hersh, *The Online Threat*, NEW YORKER, Nov. 1, 2010, at 44 (discussing the crash of a U.S. military reconnaissance aircraft over China, the resulting loss of sensitive information, and the possibility of a "cyber war" between the two nations); John Markoff & David Barboza, *Academic Paper in China Sets Off Alarms in U.S.*, N.Y. TIMES, Mar. 21, 2010, at A10 (discussing the publication of a Chinese academic paper written on the topic of attacking the United States power grid and causing it to fail).

43. *See generally* JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET? 71–81 (2006) (discussing different means by which countries may enforce Internet controls and noting the lack of any central control mechanism).

44. WikiLeaks describes itself as a "non-profit media organization" on its home page, and quotes Time Magazine for the proposition that it is a "journalistic tool." WIKILEAKS, http://wikileaks.ch (last visited Apr. 11, 2011).

Times and *Post*, employ in their newsgathering and reporting.[45] To the site's credit, it did try to engage in its own minimization procedures by contacting U.S. Ambassador Louis Susman and asking him to provide the names of individuals who would be placed at risk when WikiLeaks published the diplomatic cables.[46] The State Department, in a letter to Assange and his attorney, refused to "engage in a negotiation regarding the further release or dissemination of illegally obtained U.S. Government classified materials."[47] And, the site has published only a fraction of the cables that it purportedly holds.[48]

However, WikiLeaks has not described the criteria it uses to determine what to publish, nor what it uses to redact—if at all—information that creates risk without offsetting benefit.[49] The site does not even reveal who makes those decisions.[50] Hence, WikiLeaks' claim that "[b]etter scrutiny leads to reduced corruption and stronger democracies in all society's institutions"[51] evidently does not apply to the site itself. While journalists debate the details of their ethical system, there is considerable agreement on its core pre-

---

45. *E.g.*, Brisbane, *supra* note 19 (discussing the attempts of the *New York Times* staff to verify the WikiLeaks documents and publish them responsibly).

46. Letter from Julian Assange, Editor-in-Chief of WikiLeaks, to Louis B. Susman, U.S. Ambassador to the U.K., Nov. 26, 2010, http://www.fas.org/sgp/news/2010/11/wl-112610.pdf.

47. Letter from Harold Hongju Koh, Legal Advisor of the United States Department of State, to Jennifer Robinson, Attorney for Julian Assange, Nov. 27, 2010, http://www.foreignpolicy.com/files/fp_uploaded_documents/101129_US-Department-of-State-to-Assange-27-Nov.pdf.

48. *How Many Documents Has WikiLeaks Published?*, NPR.ORG (Dec. 28, 2010), http://www.npr.org/2010/12/28/132416904/how-many-documents-has-wikileaks-published ("Although [WikiLeaks] has vowed to publish '251,287 leaked United States embassy cables,' as of Dec. 28, 2010, only 1,942 of the cables had been released.").

49. WikiLeaks states only, "WikiLeaks has developed a harm minimization proceedure [sic] to clean documents which might endanger innocent lives. In other instances, WikiLeaks may delay publishing some news stories and their supporting documents until the publication will not cause danger to such people. However in all cases, WikiLeaks will only redact the details that are absolutely necessary to this end." *Submissions*, WIKILEAKS, http://wikileaks.ch/Submissions.html (last visited Apr. 11, 2011).

50. *E.g.*, Jim Barnett, *WikiLeaks and a Failure of Transparency*, NIEMAN JOURNALISM LAB (July 29, 2010, 10:00 AM), http://www.niemanlab.org/2010/07/wikileaks-and-a-failure-of-transparency (describing WikiLeaks as a "nonprofit journalism organization dedicated to imposing transparency on reluctant governments [that] seem to think the rules don't apply at home"); Farhad Manjoo, *The WikiLeaks Paradox*, SLATE (July 28, 2010, 4:46 AM), http://www.slate.com/id/2262066 ("Look deeply into WikiLeaks' efforts at radical transparency and you find complete opacity; WikiLeaks wants to shine a light on the world, but only by keeping itself shrouded in secrecy.").

51. *About*, WIKILEAKS, http://wikileaks.ch/About.html (last visited Apr. 11, 2011).

cepts and demands.[52] WikiLeaks not only does not discuss its normative model for publication, it does not seem to have one. The site has come under criticism from a range of journalists and scholars who have been particularly keen to contrast WikiLeaks' wide-ranging disclosure with the more measured approach, including selective redaction, taken by the five media outlets that received early access to the documents.[53]

Because WikiLeaks is not an American organization—indeed, this is part of the site's power to evade legal countermeasures—it has an attenuated connection both to the consequences of its disclosures and to the values of those effected by them. The *New York Times* was, and remains, an American media company answerable to its largely American readers, to its journalistic peers, and ultimately to American courts.[54] WikiLeaks and its controllers are responsible only to themselves and, weakly, to the cyber activists who support the site.[55] The release of documents about the conflict in

---

52. *See generally* DAVID BERRY, JOURNALISM, ETHICS AND SOCIETY (2008); THE HANDBOOK OF MASS MEDIA ETHICS (Lee Wilkins & Clifford G. Christians eds., 2009) (collecting articles on various elements of media ethics, including truth, philosophy, diversity, justice, transparency, and peace); *Code of Ethics*, SOC'Y OF PROF. JOURNALISTS, http://www.spj.org/pdf/ethicscode.pdf (last visited Apr. 11, 2011) (categorizing journalism ethics in terms of truth, reporting, the minimization of harm, independence, and accountability).

53. *See* Jay Solomon, Adam Entous & Julian E. Barnes, *Vast Leak Discloses Diplomatic Secrets,* WALL. ST. J., Nov. 29, 2010, at A1; *see, e.g.*, Russell Adams & Jessica E. Vascellaro, *To Publish Leaks or Not to Publish?*, WALL ST. J., Nov. 29, 2010, http://online.wsj.com/article/SB10001424052748703785704575643431883607708.html (noting the five international newspapers that were given advanced access to the cables: the *New York Times*, the British *Guardian*, Germany's *Der Spiegel*, the Spanish *El Pais*, and France's *Le Monde*); *see also* Stephen J.A. Ward, *Protest Attacks on WikiLeaks but Urge Responsibility*, CENTER FOR JOURNALISM ETHICS (Dec. 4, 2010), http://ethics.journalism.wisc.edu/2010/12/04/protest-attacks-on-wikileaks-but-urge-responsibility (questioning WikiLeaks' willingness to "adopt the responsible approach of the *New York Times* and *The Guardian* to their stories on the cables" and their alleged goal of minimizing harm); Jim Romenesko, *SPJ: 'Ethical Journalism Prevailed' in Reporting of Latest WikiLeaks Release*, POYNTER.ORG, (Dec. 3, 2010, 1:51 PM), http://www.poynter.org/latest-news/romenesko/109375/spj-ethical-journalism-prevailed-in-reporting-of-latest-wikileaks-release (observing that while major newspapers followed journalistic ethics in publishing information from leaked cables, WikiLeaks' intentions in publishing were more ambiguous).

54. Former *New York Times* reporter Judith Miller, for example, spent three months in prison for refusing to disclose the identity of a confidential source to a federal grand jury. *E.g.*, Adam Liptak, *Reporter Jailed After Refusing to Name Sources*, N.Y. TIMES, July 7, 2005, http://www.nytimes.com/2005/07/07/politics/07leak.html.

55. Raffi Khatchadourian, *No Secrets*, NEW YORKER, June 7, 2010, http://www.newyorker.com/reporting/2010/06/07/100607fa_fact_khatchadourian (discussing WikiLeaks' lack of accountability to traditional journalism standards and limits).

Afghanistan may benefit Afghan citizens, or the citizens of countries who contribute troops to the multinational military force fighting there.[56] But, there is no feedback loop to connect WikiLeaks' decision making to the interests of those citizens, or even to gain their views in any systematic way. One virtue of the ethical framework of journalism is that it helped the *Times* to carefully weigh the benefits to the papers' readers against the costs to those readers and to the country as a whole.[57] WikiLeaks has no rigorous, time-tested methodology for engaging in that difficult calculus, nor is it accountable in any way to those it purports to aid.[58] In consequence, the site is less useful as a check on governmental activities than standard media, such as the *Times*, which make more fine-grained, rigorous judgments about the balance between disclosure and discretion.

Thus, WikiLeaks is worrisome. There are circumstances under which information should be disclosed against a government's wishes, despite the inevitability of harm—even lost lives—that results. Media entities such as the *Times* and *Post* make such revelations regularly, as controversies over coverage of warrantless wiretapping by the National Security Agency,[59] monitoring of the SWIFT financial network,[60] and the growth of America's intelligence appa-

---

56. *See, e.g.*, Kevin Poulsen, *Wikileaks Releases Stunning Afghan War Logs—Is Iraq Next?*, WIRED (July 25, 2010, 8:40 PM), http://www.wired.com/threatlevel/2010/07/wikileaks-afghan; *Wikileaks Cables Criticise UK Military in Afghanistan*, BBC (Dec. 3, 2010), http://www.bbc.co.uk/news/uk-11906147.

57. Brisbane, *supra* note 19; s*ee also Supreme Court, 6–3, Upholds Newspapers on Publication of Pentagon Report*, N.Y. TIMES, July 1, 1971, at 1, *available at* http://www.nytimes.com/books/97/04/13/reviews/papers-final.html (discussing the Supreme Court's holding that permitted media discretion regarding what news and information implicating national security could be published).

58. *See generally* Derek E. Bambauer, *Cybersieves*, 59 DUKE L.J. 377, 400–10 (2009) (discussing accountability and assessing how closely a country's censorship aligns with the views of its citizens by examining four aspects of accountability: participation in censorship decisions, specification of authority, opportunity to challenge, and counter-majoritarian constraints).

59. 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.

60. Eric Lichtblau & James Risen, *Bank Data Is Sifted by U.S. in Secret to Block Terror*, N.Y. TIMES, Jun. 23, 2006, http://www.nytimes.com/2006/06/23/washington/23intel.html; *see* John Carroll, Mark Corallo, Bill Keller, Eric Lichtblau & John McLaughlin, *The New York Times' SWIFT Story*, PBS FRONTLINE, http://www.pbs.org/wgbh/pages/frontline/newswar/tags/swift.html (last updated Feb. 27, 2007).

ratus[61] demonstrate. But perfect disclosure is as troublesome as perfect censorship. The key question is one of process: who decides when such revelation is appropriate?[62] It is no more appropriate for a self-appointed group of cyber activists to make such choices for all Americans than for a secret government committee or a foreign government to do so. We would be troubled if, for example, the government of Iran held the power to approve or deny release of sensitive U.S. documents.[63] After all, Iran is not democratic or transparent. Its methodology for censorship decisions is arbitrary, and unmoored from American interests.[64] Yet this assessment applies equally well to WikiLeaks. No one voted for Julian Assange. The site itself resists transparency in the name of generating greater transparency—a nicely Orwellian touch. Its decisions are made with limited outside input, and there is no possibility of effective appeal of its judgments. WikiLeaks should scare us.

III. CONCLUSION

The *Pentagon Papers* case is seen as a victory because the *New York Times* was right: the paper fought a principled fight against a government that was venal, and that dramatically overstated the risks of information disclosure. However, it is likely that the *Times* was right *because of* the extraordinary steps it had to take to publish the content of the Papers. Were the publication decision entirely at the newspaper's whim, its editors and reporters might have been less judicious in their selection of materials, or less thorough in the context they provided. Process matters, as does the certainty of being judged, and possibly sanctioned, for one's decisions. The *Times*' editorial judgment operated in the shadow of legal review.

The case's principles continue to exert a gravitational force upon journalism and upon governmental regulation of journalists. Similarly, WikiLeaks hopes to play an important role in America's

---

61. Dana Priest & William M. Arkin, *A Hidden World, Growing Beyond Control*, WASH. POST, July 19, 2010, http://projects.washingtonpost.com/top-secret-america/articles/a-hidden-world-growing-beyond-control.

62. *See* Bambauer, *supra* note 58, at 380–81 (asserting that a process-oriented approach is the most appropriate method for evaluating legitimacy of censorship).

63. *See generally* ACCESS CONTROLLED 545–59 (Ronald J. Deibert, John G. Palfrey, Rafal Rohozinski & Jonathan Zittrain eds., 2010) (discussing Iranian efforts to control free speech including the legal and regulatory frameworks in place to control it).

64. *Id.* at 546.

current conflicts, and in governmental transparency more generally, by becoming the focal point for disclosure and whistle-blowing.[65] Put simply, WikiLeaks' goal is one of branding: the site hopes to be the Starbucks of leaked information. Even if the site in itself proves to be merely a curiosity—a conduit for data in a controversy that even Secretary of Defense Robert Gates described as having minimal effect on U.S. operations[66]—it will have lasting effect. WikiLeaks is an exemplar of a redistribution of power in a technological context of rapidly diminishing information costs. Media outlets, governments, and information consumers will face the WikiLeaks dilemma in recurring fashion. What action, if any, should they take in response to the availability of confidential information that carries both the potential to enlighten and to destroy?

Answering that question thoroughly is beyond the scope of this Essay. Indeed, there is no way to reverse the trend of falling information costs. (Content-based industries, such as motion picture studios and record labels, have struggled without success to do so since the advent of the Internet.[67]) But there are two initial responses worth suggesting: traditional media and force.

The *New York Times* and the *Washington Post* are viewed as the heroes of the Pentagon Papers saga. These papers, and their established counterparts in other mass media such as CNN, Fox News, Al Jazeera, and the BBC, have a critical role to play even in an information environment where consumers can bypass them and read primary sources directly. Consumers value intermediaries that add value by filtering information, providing context for it, and summarizing it.[68] We could parse the data on improvised explosive device (IED) attacks in Afghanistan from raw logs on WikiLeaks, or we can turn to the *Guardian*'s interactive map that shows where each

65. Khatchadourian, *supra* note 55.

66. Julian E. Barnes, *Gates: WikiLeaks Isn't 'Game Changer*,' WALL ST. J. (Nov. 30, 2010, 5:07 PM), http://blogs.wsj.com/washwire/2010/11/30/gates-wikileaks-isnt-game-changer.

67. *See generally* WILLIAM W. FISHER III, PROMISES TO KEEP (2004) (discussing evolving property rights and ways to regulate online entertainment as an industry); LAWRENCE LESSIG, THE FUTURE OF IDEAS (2004) (discussing the history of online entertainment, including film, music, radio, and cable TV, and the potential harms that come from the current download policies).

68. Brisbane, *supra* note 19.

attack took place.[69] Most readers still access information from a trusted gatekeeper like a newspaper, television station, or favorite blog.[70] If those intermediaries follow the example of the *New York Times* and engage in their own careful calculus about disclosure versus discretion, they can reduce the harm that results from information spills through WikiLeaks and its ilk while preserving the benefits. While this approach does not prevent malefactors from accessing information directly, it does increase costs relative to a world where the *New York Times* simply reprints unedited leaked information on the theory that it is already available. This point mirrors a lesson drawn from studies of Internet censorship: even imperfect limits can raise costs sufficiently to affect the average user's information consumption.[71] As Professor Jonathan Zittrain says, "Small fences keep in large mammals."[72]

Next, governments, including America's, may need to re-think enforcement. Ultimately, a state's legal jurisdiction is demarcated by the boundaries of its ability to enforce judgments.[73] As discussed, Internet technology complicates enforcement; sites such as WikiLeaks can exist in multiple, friendly jurisdictions.[74] The ease with which bits cross borders, and the near-zero cost of those bits, cuts both ways, though. Interdiction via code—a cyberattack—is nothing more than information directed at a particular computer.[75] Locating WikiLeaks in Switzerland may prevent American police from interfering, but it does nothing to prevent American code from operating there. The data spill of U.S. diplomatic cables did not war-

---

69. Mark McCormick, Paddy Allen & Alastair Dant, *Afghanistan War Logs: IED Attacks on Civilians, Coalition and Afghan Troops*, GUARDIAN (LONDON), July 26, 2010, http://www.guardian.co.uk/world/datablog/interactive/2010/jul/26/ied-afghanistan-war-logs.

70. *See, e.g.*, Steven Hoffer, *Study: Social Media Closing in on Newspaper Websites*, AOL NEWS (Aug. 13, 2010, 5:09 PM), http://www.aolnews.com/2010/08/13/study-social-media-closing-in-on-newspaper-websites (citing newspaper websites and social media as popular sources of news).

71. *See generally* Bambauer, *supra* note 23.

72. Donna Wentworth, *Lessig & Zittrain on Regulating Speech*, COPYFIGHT (May 13, 2004), http://copyfight.corante.com/archives/003648.html.

73. *See* Robert Cover, *Violence and the Word*, 95 YALE L.J. 1601, 1618–19 (1986) (describing the role of judges as being interconnected with other actors in the judicial system including, but not limited to, legislators, enforcers, guards, and other citizens).

74. *See, e.g.*, Khatchadourian, *supra* note 55 (stating that WikiLeaks has more than twenty servers in jurisdictions around the world and hundreds of domain names).

75. *See* Bambauer, *supra* note 23; Herbert S. Lin, *Offensive Cyber Operations and the Use of Force*, 4 J. NAT'L SECURITY L. & POL'Y 63, 63 (2010).

rant aggressive measures from the American government,[76] but future revelations might. Even cyberattacks that were only partially effective would have the desired outcome of raising the cost of accessing information. WikiLeaks' redundancy, while considerable, is only a partial answer: the site must advertise its accessibility.[77] Readers have to know how to find WikiLeaks. This means attackers can know how to find WikiLeaks as well.

The key issue is deciding the criteria for employing technological measures against a distribution mechanism like WikiLeaks. In short, when should the government launch an attack? Clearly the importance of the information at stake is one consideration; but, there are other considerations.[78] Any attack can have unintended consequences, particularly when it must travel across neutral networks to reach the target. Technical countermeasures can also have perceptual repercussions. Most countries criminalize hacking.[79] If the United States hacks infrastructure owned and operated by non-state actors there could be consequences for the perceived legitimacy of the action,[80] and for America's ability to object to hacking in the future. To date, United States policy on offensive cyber actions has remained largely secret and, when it has become public, almost entirely opaque.[81] While the government's wariness in discussing its capa-

---

76. *Cf.* Near v. Minnesota, 283 U.S. 697, 716 (1931) (stating that in wartime, "a government might prevent actual obstruction to its recruiting service or the publication of the sailing dates of transports or the number and location of troops"); United States v. Progressive, Inc., 467 F. Supp. 990, 993–95 (W.D. Wis. 1979) (preventing publication of hydrogen bomb technical specifications where there existed a close temporal relationship to conflict).

77. *See* Doug Aamoth, *WikiLeaks Domain Name Killed (and Why It Won't Kill WikiLeaks)*, TECHLAND (Dec. 3, 2010), http://techland.time.com/2010/12/03/wikileaks-domain-name-killed-and-why-it-wont-kill-wikileaks (stating that WikiLeaks is still accessible via alternative domain names and, as long as the site is connected to the Internet, people can access WikiLeaks using the IP address).

78. *Cf.* Jane Yakowitz, *The Tragedy of the Data Commons*, 25 HARV. J.L. & TECH. __ (forthcoming 2012) (describing tradeoffs in making anonymized data sets available for research).

79. *See, e.g.*, Council Framework Decision 2005/222/JHA of 24 Feb. 2005 on Attacks Against Information Systems, art. 6, 2005 O.J. (L 69) 67, 67, *available at* http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:069:0067:0071:EN:pdf.

80. *See, e.g.*, Europ. T.S. No 185, art. II, IV, V, *Convention on Cybercrime* (2001), *available at* http://conventions.coe.int/Treaty/en/Treaties/html/185.htm.

81. *See* U.S. DEP'T OF DEF., QUADRENNIAL DEFENSE REVIEW REPORT 37–41 (2010), *available at* http://www.defense.gov/qdr/images/QDR_as_of_12Feb10_1000.pdf (discussing suggested protocols for operating effectively in cyberspace, including increased knowledge and interdepartmental cooperation); Ellen Nakashima, *Pentagon's Cyber Command Seeks Authority to Expand Its Battlefield*, WASH. POST, Nov. 6, 2010, http://www.washingtonpost.com/wp-

bilities and framework for launching cyberattacks is understandable, so far it has been in the context of a conflict between states.[82] It might be necessary to employ cyber countermeasures against a civilian intermediary like WikiLeaks. Since such intermediaries have limited capability to respond (the denial-of-service attacks launched by the hacktivist group "Anonymous" on WikiLeaks' behalf against MasterCard, PayPal, and Amazon were noisy but ineffective[83]), the United States does not need to fear losing further deterrence by publicly debating its options.[84] The government should do so. Having the capability to interdict WikiLeaks is vital to restoring a state's enforcement power. Furthermore, establishing guidelines for when to employ that force will increase the legitimacy of doing so.

In the end, it is easy to draw a line that runs from the *Pentagon Papers* case through the WikiLeaks saga, pointing towards an era of greater transparency, openness, and access—where governments are held accountable through disclosure whether they consent or not. Such a belief is attractive, but also false. The better world is one where the censor can win, where the balance of benefits versus harms occurs in public, based on established principles and not on whim. It matters not only that the *New York Times* bested the Nixon administration, but that the contest was an uncertain one for both sides, ultimately resolved by a disinterested intermediary with the

---

dyn/content/article/2010/11/05/AR2010110507304.html (observing the ambiguous and vague statements made by public officials regarding cyber-operations). *See generally* TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES (William A. Owens, Kenneth W. Dam & Herbert S. Lin eds., 2009).

82. *E.g.*, U.S. DEP'T OF DEF., *supra* note 81, at iv, vi (stating that non-state actors will continue to grow increasingly influential and that the government must be able to work with them, while also prevailing over other state aggressions).

83. *See Pro-Wikileaks Activists Abandon Amazon Cyber Attack*, BBC NEWS (Dec. 9, 2010, 6:31 PM), http://www.bbc.co.uk/news/technology-11957367 (determining that the attacks were one method to keep WikiLeaks, and its information, in the public eye); Sarah Perez, *As Attacks on PayPal, Amazon Fail, Anonymous Wikileaks Supporters Begin "Operation LeakSpin"*, READWRITEWEB (Dec. 10, 2010, 8:20 AM) http://www.readwriteweb.com/archives/as_attacks_on_paypal_amazon_fail_anonymous_wikilea.php (stating that the attacks run by Anonymous were disorganized and appeared to fail).

84. *See generally* Mark D. Young, *National Cyber Doctrine: The Missing Link in the Application of American Cyber Power*, 4 J. NAT'L SECURITY L. & POL'Y 173, 185–89 (2010) (stating that the new cyber policy should be unclassified to the greatest extent possible and discussed nationally among the government and private sectors to ensure the new policy has the best foundation, training, integration, and coordination of resources to combat cyberattacks).

power to enforce its decision. WikiLeaks is a cautionary tale, one that will recur. It teaches that the right lesson from the *Pentagon Papers* case is—consider the censor. Some information should not be disclosed, and we should pay heed to who makes that determination.