

“THE ASSANGE EFFECT”: WIKILEAKS, THE ESPIONAGE ACT AND THE FOURTH ESTATE

By Shaina Jones and Jay Ward Brown¹⁸

¹⁸ Ms. Jones is an associate and Mr. Brown is a partner in Levine Sullivan Koch & Schulz, LLP, a firm specializing in media law with offices in Washington, D.C., New York City, Philadelphia and Denver. Summer intern Sean McKibben contributed to the preparation of this article.

In the wake of the November 2010 publication of thousands of highly-classified diplomatic cables, the “whistle-blowing”¹ website WikiLeaks has prompted an international debate on, among other matters, possible prosecution of the organization or its leader under the American Espionage Act.² Indeed, a grand jury empanelled by the United States government apparently is considering whether to indict WikiLeaks Editor-in-Chief Julian Assange as the result of his organization’s publication of the cache of diplomatic cables. Return by the grand jury of such an unprecedented indictment would present fundamental questions regarding the contours of protection for the press under the First Amendment to the U.S. Constitution.

While other of its provisions criminalize traditional “spying,” such as the unauthorized entry into or electronic surveillance of military facilities and the delivery to foreign nations of defense-related information likely to be injurious to the U.S.,³ the provisions of the Espionage Act most often cited as potentially applicable to WikiLeaks make it unlawful to:

(1) “receive or obtain” from “any person or any source whatever,” any “information respecting the national defense with intent or reason to believe that the information is to be used to the injury of the United States, or to the advantage of any foreign nation” while knowing or having reason to believe that the source of the information was providing it in violation of the Act;⁴

(2) have “unauthorized possession of” a document “relating to the national defense” with “reason to believe [the information] could be used to the injury of the United States or to the advantage of any foreign nation” and “willfully communicate” it to “any person not entitled to receive it;”⁵ and

(3) to conspire with another person to do any of the foregoing if any member of the conspiracy does “any act to effect the object of the conspiracy.”⁶

Persons convicted under these provisions of the Espionage Act are subject to imprisonment and monetary fine.

1 Delia Lloyd, *WikiLeaks, Whistleblowing and the Future of Journalism*, POLITICS DAILY (Jan. 31, 2011), <http://aol.it/hhReA1>. (The authors have provided shortened “bit.ly” web addresses for ease of use.)

2 18 U.S.C. § 793.

3 *Id.* at § 793(a)-(b).

4 *Id.* at § 793(c).

5 *Id.* at § 793(e).

6 *Id.* at § 793(g).

This paper examines what might be required to sustain a prosecution of Assange under the Espionage Act and the possible legal impact of such a prosecution on traditional news organizations. In Part I, we briefly trace Assange’s biography and provide an overview of WikiLeaks. In Part II, we discuss the history of and public policy behind the Espionage Act, and examine what the government would be required to prove in order successfully to prosecute Assange, including whether the First Amendment might provide a defense to such a prosecution. In Part III, we briefly consider how prosecution of Assange might differ under the Official Secrets Act in Great Britain (on which the American Espionage Act is in part based) if the leaked materials had belonged to the British government. Finally, in Part IV, we consider how the WikiLeaks affair has affected newsgathering more generally, including the adoption by some mainstream media organizations of information-gathering apparatus similar to that employed by WikiLeaks.

I. ASSANGE AND WIKILEAKS: A BRIEF HISTORY

A. The Emergence Of Julian Assange

Relatively little is known about Julian Assange before his public association with WikiLeaks in 2007, and the public record contains accounts of both his past and recent activities that are in some respects contradictory. Few photographs exist to document his early upbringing and the now 40-year-old is known to be wary of face-to-face interviews. However, his earlier life does seem to have presaged the itinerant nature of his role as WikiLeaks’ editor-in-chief.

Assange was born in 1971 in Townsville, Australia. His mother and stepfather ran a touring theatre, which seems to have introduced Assange to the nomadic life early on. By the time he reached the age of 14, Assange reportedly had moved 37 times and attended more than 30 schools.⁷ He eventually settled at the University of Melbourne, where he studied mathematics and physics, and developed an interest in computer technology. In September 1991, at age 20, Assange was charged with hacking into Canadian telecom giant Nortel. Fearing prison, he pled guilty to 24 of 31 criminal charges and was fined approximately \$2,000.⁸

His mother has described Assange as “highly intelligent,” and “too smart for himself,” while his stepfather has said that he was “a very bright boy with a keen sense of right and wrong” and a “sharp kid who always fought for the underdog.”⁹ Confidant Daniel Schmitt similarly has described Assange as “one of the few people who really care about positive reform in this world to a level where you’re willing to do something radical to risk making a mistake,

⁷ Raffi Khatchadourian, *No Secrets, Julian Assange’s mission for total transparency*, THE NEW YORKER (June 7, 2010), <http://nyr.kr/b7yueB>.

⁸ Luiza Savage, *Julian Assange: The man who exposed the world*, MCCLEAN’S (Dec. 27, 2010), <http://bit.ly/eMSyMK>.

⁹ *The secret life of Julian Assange*, CNN.COM (December 2, 2010, 3:10 pm EST), <http://bit.ly/dYXp9e>.

just for the sake of working on something they believe in.”¹⁰ By the same token, Assange also has been described by an interviewer as absent-minded:

He can concentrate intensely, in binges, but he is also the kind of person who will forget to reserve a plane ticket, or reserve a plane ticket and forget to pay for it, or pay for the ticket and forget to go to the airport. People around him seem to want to care for him; they make sure that he is where he needs to be, and that he has not left all his clothes in the dryer before moving on. At such times, he can seem innocent of the considerable influence that he has acquired.¹¹

In December 2010, Assange was arrested in the United Kingdom on a Swedish warrant issued in connection with alleged sex offenses, charges he vehemently denies. Assange currently is under house arrest in England, awaiting appellate proceedings regarding possible extradition to Sweden.¹² Before his December arrest, Assange was by most accounts a nomad, “traveling from country to country, staying with supporters, or friends of friends,”¹³ with very few belongings. Indeed, it appears largely to be the case that WikiLeaks existed wherever he did.¹⁴ Mr. Assange explained during an interview conducted by Swiss artist Hans Ulrich Obrist why he believes his nomadic lifestyle is necessary to his role as head of WikiLeaks:

“I’ve been traveling all over the world on my own since I was twenty-five, as soon as I had enough money to do it. But for WikiLeaks, I have been consistently on the move since the beginning of 2007. . . . It was more about following opportunity and ensuring that I wasn’t in one place long enough to allow for a proper surveillance operation, which involves getting inside and installing video cameras, monitoring all outgoing electronic signals, and so forth. Such operations take time and planning, so if you’re a resource-constrained activist organization facing the prospect of surveillance by some of the most advanced surveillance agencies, such as the National Security Agency and GCHQ, you only have two methods to resist it: one, changing the location of your headquarters with some frequency, and two, complete geographic isolation.”¹⁵

10 *Profile: WikiLeaks founder Julian Assange*, BBC (December 7, 2010), <http://bbc.in/aTzVw7>.

11 Khatchadourian, *supra* note 8.

12 *Times Topics, Julian Assange*, N.Y. TIMES (February 24, 2011), <http://nyti.ms/dGQzm5>.

13 Khatchadourian, *supra* note 8.

14 *Id.*

15 *In Conversation with Julian Assange Part II*, WIKILEAKS (June 15, 2011), <http://wikileaks.org/In-Conversation-with-Julian,107.html>.

To ensure the sustainability of WikiLeaks, Assange says, he chose the former.

B. The Advent And Rapid Ascent of WikiLeaks

Described on its current website as “a non-profit media organization dedicated to bringing important news and information to the public,” the Internet domain WikiLeaks.org was registered on October 4, 2006. The creators of WikiLeaks have never been formally identified, and the organization claimed only vaguely that it was formed by “Chinese dissidents, journalists, mathematicians and start-up company technologists from the U.S., Taiwan, Europe, Australia and South Africa.”¹⁶ Although Julian Assange has described himself as merely a member of the organization’s governing board, in fact, he has been its public face since 2007. Beyond Mr. Assange and a handful of senior associates, the organization and its now-famous website appear heavily dependent on what it claims are some 800 designated occasional volunteers. Operating with what it has said is an annual budget of £175,000, WikiLeaks apparently relies solely on donations for its operating funds.¹⁷

Just as the Internet has no physical address or main office, neither does WikiLeaks.¹⁸ WikiLeaks has no official headquarters, and apparently has neither paid staff (some are known only by their initials) nor physical offices.¹⁹ It operates its primary computer server in Sweden, where on-line anonymity is protected by law. Recently, WikiLeaks moved its main, secure server to Pionen, a former civil defense center located in bedrock deep under the city of Stockholm and now used by an ISP as a secure data storage facility. Communications within WikiLeaks are conducted in encrypted chat rooms.²⁰

The organization published its first leaked document just two months after it registered the WikiLeaks domain, in December 2006. The document was a “secret decision” signed by Sheikh Hassan Dahir Aweys, a Somali rebel leader for the radical Islamic Courts Union,²¹ and called for the hiring of hit men to carry out the planned assassinations of government officials.²² Assange has admitted that he was uncertain of the authenticity of the Islamic Courts Union document, but that he nevertheless released it because of his belief that readers of the site, using

16 Alex Altman, *A Coming Chill Over Internet Freedom?*, TIME.COM (Feb. 20, 2008), <http://ti.me/85wNL3>.

17 See WIKILEAKS, <http://wikileaks.org/Donate.html>.

18 Jay Rosen, *The Afghanistan War Logs Released by Wikileaks, the World’s First Stateless News Organization*, PRESS THINK (July 26, 2010), <http://bit.ly/9eGbHD>.

19 Khatchadourian, *supra* note 8.

20 *Id.*

21 *SOMALIA: Islamic courts set up consultative council*, IRIN (June 26, 2006), <http://bit.ly/r10i0U>.

22 *WikiLeaks: Spy for the little guy*, ALJAZEERA (Oct. 23, 2010, 10:34 GMT), <http://aje.me/bsrih2>.

“wiki” functions, would help edit, analyze and authenticate it.²³ The authenticity of the Islamic Courts Union document remains uncertain, but soon after its posting, news about WikiLeaks surpassed interest in the document itself.²⁴ With more recent releases of documents, WikiLeaks has moved from its original, user-edited model to a more traditional model of publication that is not open for editing by visitors to the website.

Indeed, WikiLeaks has amassed an expansive catalogue of secret, top-secret and confidential documents since its launch in 2006. In August 2007, on the basis of a leaked document provided by WikiLeaks, the British newspaper *The Guardian* published a story detailing corruption in the family of Kenyan leader Daniel Arap Moi. The leaked document, a report created by the international risk assessment firm Kroll, uncovered abuses by Moi, his family and his associates relating to almost \$3 billion of government funds. The disclosure placed Kenya, the Democratic Republic of the Congo and Nigeria at the forefront of further news reporting of extensive corruption,²⁵ and WikiLeaks received an award from Amnesty International for its work.²⁶ Just three months later, in November 2007, WikiLeaks published 238 pages of documents comprising U.S. Army Standard Operating Procedures in use at the Guantanamo Bay detention center in 2003. The documents, which were unclassified but designated “for official use only,” included schematics of the camp; detailed checklists of “comfort items,” such as extra toilet paper, that could be given to detainees as rewards; instructions for processing new detainees and how to manipulate them psychologically; and rules for dealing with hunger strikes. The documents also revealed that some prisoners were kept off-limits to the International Committee of the Red Cross, charges that that the U.S. military had publicly denied.²⁷

By 2008, WikiLeaks had released several other documents, including documents which raised allegations of fraud on the part of the Swiss Bank; the “secret bibles” of the Church of Scientology; and contents of a Yahoo account belonging to former U.S. vice-presidential candidate Sarah Palin.²⁸

In 2009, among other documents, the site released 86 intercepted telephone recordings of Peruvian politicians and businessmen involved in the 2008 Peru oil scandal; internal documents from Kaupthing Bank shortly before the collapse of Iceland’s banking sector; a British document

23 Khatchadourian, *supra* note 8. This explains the organization’s name: The term “wiki” refers to the type of website that allows visitors to freely edit and add links to a webpage, creating a collaborative user experience. See <http://www.merriam-webster.com/dictionary/wiki>.

24 Khatchadourian, *supra* note 8.

25 Xan Rice, *The looting of Keyna*, THE GUARDIAN (Aug. 3, 2007), <http://bit.ly/hkzZzr>.

26 Lucy Kennedy, *5 Things You Need To Know About WikiLeaks*, PBS (July 7, 2010), <http://to.pbs.org/cr3BBf>.

27 Jane Sutton, *Guantanamo operating manual posted on Internet*, REUTERS (Nov. 14, 2007, 6:54 pm EST), <http://reut.rs/e5C9Bc>.

28 Kim Zetter, *Group Posts E-Mail Hacked From Palin Account — Update*, WIRED (Sept. 17, 2008, 9:50 am), <http://bit.ly/6Qqg47>.

advising its security services on how to avoid documents being leaked; and 570,000 intercepts of pager messages sent on the day of the September 11 attacks in the United States.²⁹

Clearly, however, of all WikiLeaks' disclosures, the most notorious concern the United States. In April 2010, WikiLeaks released "Collateral Murder," a classified video of a July 12, 2007 airstrike by an Apache helicopter firing on and killing a group of civilians that included two Reuters journalists.³⁰ In July 2010, the site released the "Afghanistan War logs," containing 92,000 field memos from the Afghanistan war, dating from 2004 through the end of 2009.³¹ In October 2010, WikiLeaks released the "Iraq War logs," consisting of almost 400,000 field memos that include, among other things, descriptions of instances of torture and execution and civilian death statistics.³² A month later, WikiLeaks published the first of 251,287 confidential diplomatic cables, providing a rare insight into the inner workings and opinions of United States diplomats.³³ In April 2011, the site published more than 700 classified reports on current and former prisoners at the Guantanamo Bay prison facility, which apparently include new details on the location and organization of al-Qaida members before and after the September 11 attacks.³⁴

In an interview with *Forbes*, Assange spoke about the future, saying, "We have one [leak] related to a bank coming up, that's a 'megaleak.'"³⁵ While WikiLeaks has made no further official comment on this subject, public speculation has focused on Bank of America, not least because of Bank of America's decision in December 2010 to stop accepting credit card transactions for donations to WikiLeaks, and because published reports have said that Bank of America has recruited the consulting firm Booz Allen Hamilton³⁶ and the law firm Hunton & Williams³⁷ to assist it with unspecified issues.

29 Declan McCullagh, *Egads! Confidential 9/11 Pager Messages Disclosed*, CBS NEWS (Nov. 25, 2009, 10:00 am), <http://bit.ly/mPSiqo>.

30 Elisabeth Bumiller, *Video Shows U.S. Killing of Reuters Employees*, N.Y. TIMES (April 5, 2010), <http://nyti.ms/qQ9pfW>.

31 *Afghanistan war logs: the unvarnished picture*, THE GUARDIAN (July 25, 2010, 22:04 BST), <http://bit.ly/bwn2hC>.

32 Adam Brookes, *Huge WikiLeaks release shows US 'ignored Iraq torture'*, BBC (October 23 2010, 5:42 ET), <http://bbc.in/dxz1gV>.

33 Andrew Lehren & Scott Shane, *Leaked Cables Offer Raw Look at U.S. Diplomacy*, N.Y. TIMES (Nov. 28, 2010), <http://nyti.ms/hfyORk>.

34 *WikiLeaks publishes Guantanamo detainee documents*, CNN.COM (Apr. 24, 2011), <http://bit.ly/mTJ0AL>.

35 Andy Greenberg, *An Interview With WikiLeaks' Julian Assange*, FORBES (Nov. 29, 2010, 5:02 p.m.), <http://onforb.es/ia0bZW>.

36 Nelson D. Schwartz, *Facing Threat From WikiLeaks, Bank Plays Defense*, N.Y. TIMES (Jan. 2, 2011), <http://nyti.ms/ebigqv>.

37 Eric Lipton & Charlie Savage, *Hackers Reveal Offers to Spy on Corporate Rivals*, N.Y. TIMES (Feb. 11, 2011), <http://nyti.ms/qsdNa4>.

The diplomatic cables, war logs, and “Collateral Murder” video all allegedly were made available to WikiLeaks by a single U.S. Army private, Bradley Manning. In May 2010, just after the release of the video, a person identifying himself as Manning described in an on-line chat room various materials he claimed to have downloaded, including “State Department cables from embassies and consulates all over the world.” During this on-line chat session with Adrian Lamo, an admitted computer hacker, the person indentifying himself as Manning claimed that he had delivered the materials to WikiLeaks. Lamo would later report Manning to authorities, which led to his arrest at the end of May 2010.³⁸

In connection with the leak of the “Collateral Murder” video, Manning has been charged with various offenses under Articles 92 and 134 of the Uniform Code of Military Justice (“UCMJ”), including:

- illegal transfer of classified data to his personal computer;
- adding unauthorized software to a classified computer system; and
- communicating, transmitting and delivering national defense information to an unauthorized recipient with reason to believe such disclosure could cause injury to the United States.³⁹

In March of 2011, 22 additional charges under the UCMJ were filed against Manning, specifically in connection with the leaked war logs and State Department cables. The new charges include aiding the enemy, a capital offense (and a charge that has prompted debate as to which “enemy” Manning is accused of aiding),⁴⁰ and that Manning violated section 793(e) of the Espionage Act. As noted above, section 793(e) makes it unlawful for a person “having unauthorized possession of . . . any document . . . relating to the national defense” with “reason to believe [the information] could be used to the injury of the United States or to the advantage of any foreign nation” to “willfully communicate[it] . . . to any person not entitled to receive it.”⁴¹

For the moment, Manning remains the only person charged in connection with these events. As the government doubtless realizes, to prosecute a soldier for disseminating classified information is one thing. Prosecuting a civilian or a civilian organization that received and then disseminated that same information to the public is another. Yet the question remains whether this might be the circumstance in which the government is prepared to make this particular leap.

38 *Times Topics: Bradley Manning*, N.Y. TIMES (Mar. 3, 2011), <http://nyti.ms/n3d5zh>.

39 <http://graphics8.nytimes.com/packages/pdf/world/2010/Manning-charge-sheet.pdf>.

40 *WikiLeaks: Bradley Manning faces 22 new charges*, CBS NEWS (Mar. 2, 2011, 6:39 pm ET), <http://bit.ly/r8in72>.

41 18 U.S.C § 793(e); *see also Bradley Manning: charge sheet*, THE GUARDIAN (Mar. 4, 2011), <http://bit.ly/iibcNd>.

II. THE ESPIONAGE ACT AND ASSANGE: AN EVOLVING PERSPECTIVE

A. The Espionage Act's Precursors

The current U.S. Espionage Act traces its roots at least back to the Sedition Act of 1798. Officially titled “An Act for the Punishment of Certain Crimes Against the United States,”⁴² the 1798 Sedition Act criminalized the making of “false, scandalous and malicious” writings about the federal government.⁴³ Ostensibly adopted for the purpose of strengthening the national morale during an undeclared naval war with France, the Sedition Act served as a political tool in the hands of the governing Federalist party to silence the Republican dissent.⁴⁴ Federalists enforced the Sedition Act with some vigor, launching prosecutions against four of the five most influential Republican journals and many smaller Republican newspapers, some of which folded when their editors were jailed.

The Sedition Act expired according to its terms in the spring of 1801, on the last day of the presidency of the Federalist John Adams. This “coincidence” of timing has been cited by those who argue that the Act was intended purely as a political tool from the time of its introduction in Congress, and that it was carefully crafted so that it could not be applied by Republicans to Federalist publications if Republicans gained control of the Executive Branch. What is undisputed is that, after the Act’s expiration in 1801, the United States survived (some might say “thrived”) for more than a century with no limitation under federal law on “seditious” expression.

More immediately, the Espionage Act of 1917 was based on the Defense Secrets Act of 1911, which, as its name implies, criminalized the disclosure of defense-related secrets (and was itself based on the then-current version of the British Official Secrets Act). Passage of the Act was in part reaction to the propaganda machines used to such dramatic effect by European powers and Russian rebels during World War I. Attorney General Thomas Gregory argued that the federal government needed new and broader tactics to restrict “warfare by propaganda.”⁴⁵ President Wilson concurred, asserting in an address to Congress the “need for legislation to suppress disloyal activities.”⁴⁶ With the ostensible purpose of addressing concerns of the military, legislation that would become the Espionage Act was introduced in early 1917 and purported to criminalize that which “endangered the peace, welfare, and honor of the United

42 *Public Acts of Fifth Congress, Second Session, Ch. 74, Stat. 596*, LIBRARY OF CONGRESS, <http://1.usa.gov/4KnXdf>.

43 *Id.*

44 See GEOFFREY R. STONE, *PERILOUS TIMES: FREE SPEECH IN WARTIME FROM THE SEDITION ACT OF 1798 TO THE WAR ON TERRORISM*, 43 (2004).

45 DEPARTMENT OF JUSTICE, *ANNUAL REPORT OF THE ATTORNEY GENERAL OF THE UNITED STATES FOR THE YEAR 1918*, 16-17 (1918)

46 DAVID M. KENNEDY, *OVER HERE: THE FIRST WORLD WAR AND AMERICAN SOCIETY*, 24 (1980)

States.”⁴⁷ After nine weeks of debate, Congress approved the legislation on June 15, 1917. It bears note that, shortly thereafter, Congress expanded the Espionage Act through the Sedition Act of 1918, which criminalized, among other things, the use of “disloyal, profane, scurrilous or abusive language” about the United States.⁴⁸ This return to “sedition” was short-lived, however, as the Sedition Act amendments were repealed approximately two years later.

B. Historical Application of the Espionage Act

There were nearly two thousand prosecutions and more than a thousand convictions under the Espionage Act of 1917, the vast majority of both involving provisions that criminalized, during time of war, the making of statements intended to interfere with the success of U.S. military operations or to promote the success of American enemies.⁴⁹ During the early part of the 20th century, defendants routinely received stringent punishment for various “disloyal” acts. Among the most notable individuals indicted under the Act were Socialist Party leader Eugene V. Debs and others from the Industrial Workers of the World (IWW), then the largest industrial union in the United States. Debs was notorious for his speeches against World War I and President Woodrow Wilson, who called Debs “a traitor to his country.” Ultimately, Debs was sentenced to 10 years in prison for his rhetoric.⁵⁰ Additionally, in *Shaffer v. United States*,⁵¹ the defendant was charged under the Act for possessing and mailing copies of the book, “The Finished Mystery,” in which the author stated of World War I that “[t]he war itself is wrong. Its prosecution will be a crime. There is not a question raised, an issue involved, a cause at stake, which is worth the life of one blue-jacket on the sea or one khaki coat in the trenches.” Shaffer was convicted under the Act, and the U.S. Court of Appeals for the Ninth Circuit affirmed his conviction. In a similar suppression of criticism of World War I, in *United States v. Motion Picture Film “The Spirit of ‘76,”*⁵² a federal court upheld the seizure by the government of a film about the Revolutionary War because it portrayed “objectionable” scenes of cruelty by British soldiers and therefore could create “animosity or want of confidence” between the then-allies Great Britain and the U.S. The producer of the film also was convicted under the Act. And in *O’Hare v. United States*,⁵³ the court affirmed the conviction and five-year sentence of Kate Richards O’Hare, an American activist who had said in a speech in North Dakota, “any person who enlisted in the army of the United States for service in France would be used for fertilizer,

47 Jareen Trudell, *The Constitutionality of Section 793 of the Espionage Act and Its Application to Press Leaks*, 33 WAYNE L. REV. 205, 205-206 (1986) (citing 55 CONG. REC. 1695 (1917)).

48 *The Sedition Act of 1918, From the United States Statutes at Large, Vol. 40 (April 1917-March 1919)*, PBS, <http://to.pbs.org/pqgo7n>.

49 DAVID M. RABBAN, FREE SPEECH IN ITS FORGOTTEN YEARS, 256 (1999)

50 *Debs v. United States*, 249 U.S. 211 (1919).

51 255 F. 886, 886 (9th Cir. 1919).

52 252 F. 946 (S.D. Cal. 1917).

53 253 F. 538 (8th Cir. 1918).

and that is all he was good for, and that the women of the United States were nothing more nor less than brood sows, to raise children to get into the army and be made into fertilizer.”

Given the origins of the Espionage Act, it perhaps is not surprising that significant judicial construction of its terms took place during and immediately following World War II. In *Gorin v. United States*,⁵⁴ for example, Mikhail Gorin, a citizen and agent of the USSR, was shown to have bought information from a U.S. Navy employee, Hafis Salich, about Japanese activities in the United States. The reports were in the files of the Naval Intelligence branch office at San Pedro, California, and concerned the activities of Japanese officials and civilians within the U.S., as well as American surveillance of Japanese vessels suspected of engaging in espionage. Gorin and Salich were convicted under the criminal prohibitions against classic “spying” and for conspiracy.

On appeal to the U.S. Supreme Court, Gorin and Salich argued that the reach of the statute was limited to information concerning the specific military facilities and equipment named in the statute, and that to construe the Act more broadly would render it unconstitutionally vague because citizens would need to guess what information was sufficiently related to the national defense to trigger the Act’s prohibitions, thereby chilling public dialogue about important matters of governance. The Court rejected these contentions, holding that the concept of “national defense” is not limited under the Act to the specifically named places and things and that, while broad in scope, the term is sufficiently clear to guide the conduct of citizens and will not chill political speech.⁵⁵ In particular, the Court observed that the scienter requirement in the statute has the effect of narrowing the class of “national defense information” to which the Act may be applied, since by definition such scienter can arise only with respect to secret (as opposed to publicly available) information:

The obvious delimiting words in the statute are those requiring “intent or reason to believe that the information to be obtained is to be used to the injury of the United States, or to the advantage of any foreign nation.” This requires those prosecuted to have acted in bad faith. The sanctions apply only when scienter is established. Where there is no occasion for secrecy, as with reports relating to national defense, published by authority of Congress or the military departments, there can, of course, in all likelihood be no reasonable intent to give an advantage to a foreign government.⁵⁶

The convictions were affirmed.

⁵⁴ 312 U.S. 19 (1941).

⁵⁵ *Id.* at 21 n.1; *see also id.* at 25-26.

⁵⁶ *Id.* at 27-28 (footnotes omitted).

Just five years later, the Court had another opportunity to outline the requirements for prosecution under the Act in *Hartzel v. United States*⁵⁷ Unlike Gorin, however, Elmer Hartzel was a civilian, not a government agent or employee. In 1942, Hartzel wrote three articles expressing his negative opinion of World War II and the Allies, among other things. For example, in his pamphlet titled “The Diseased Spinal Cord,” Hartzel wrote the following about President Roosevelt:

“Wilson died an invalid; Roosevelt became president one. What is the social significance of his condition? . . . Our leader—safe in Washington—escaped the actual horrors of war, but he could not escape the virus of a child’s disease. As with syphilis his paralysis is indicative of severe maladjustments within the nation. He reproduces within his body our internal breakdown; he is in fact a degenerate who now seeks ways of having us cure him of his ailment. . . . Hidden within the present program to save humanity are germs of infantilism, paralysis and death. For we now follow, not a little child, but a man with a child’s disease.”⁵⁸

Hartzel distributed his writings to some six hundred addresses gleaned from his mailing list.

The prosecution claimed that Hartzel’s conduct fell within the scope of a provision of the Espionage Act that criminalized causing or attempting to cause “insubordination, disloyalty, mutiny, or refusal of duty, in the military or naval forces of the United States,” and obstructing “the recruiting or enlistment service of the United States, to the injury of the service or the United States.”⁵⁹ The Supreme Court held that the government had failed to establish the requisite intent—in this case, “specifically to cause insubordination, disloyalty, mutiny or refusal of duty in the military forces or to obstruct the recruiting and enlistment service.”⁶⁰ Accordingly, the Court announced that, “[u]nless there is sufficient evidence from which a jury could infer beyond a reasonable doubt that he intended to bring about the specific consequences prohibited by the Act, an American citizen has the right to discuss these matters either by temperate reasoning or by immoderate and vicious invective without running afoul of the Espionage Act of 1917.”⁶¹ Because Hartzel was attempting to change public opinion about the war based on his personal views, the Court concluded that he could not be convicted under the Act.

⁵⁷ 322 U.S. 680 (1944).

⁵⁸ *United States v. Hartzel*, 138 F.2d 169, 171 (7th Cir. 1943) (quoting pamphlet), *rev’d on other grounds by Hartzel v. United States*, 322 U.S. 680 (1944).

⁵⁹ *Hartzel*, 322 U.S. at 686 (quoting Section 3 of the Act).

⁶⁰ *Id.* at 687.

⁶¹ *Id.* at 689.

More recently, in 1988, the U.S. Court of Appeals for the Fourth Circuit examined the reach of the Espionage Act in a press-related context in *United States v. Morison*.⁶² Samuel Morison was an employee at the Naval Intelligence Support Center who also worked off-duty as a paid consultant to *Jane's*, the English publisher of various defense-related periodicals. For some period, Morison supplied various photographs and information to *Jane's* with the Navy's approval, but subject to Morison's agreement that he would not supply classified information. When Morison's off-duty services to *Jane's* became a source of friction with his Naval superiors, Morison interviewed for permanent employment with *Jane's*. Possibly in the hope of securing the job, Morison subsequently mailed various classified photographs to *Jane's* editor in chief, which the magazine published.⁶³ While *Jane's* never was charged, Morison was indicted and convicted under, among other criminal statutes, sections 793(d) and (e) of the Espionage Act, which make it unlawful for those having lawful or unlawful possession of national defense information with reason to believe it could be used to the detriment of the U.S. or the benefit of its enemies to willfully communicate it to any person not entitled to receive it. In his defense, Morison sought to cast himself in the guise of a news source, and argued that the Act did not apply to him because he did not fit the profile of a "classic spy." The Fourth Circuit rejected this contention, observing that the sections of the Espionage Act under which Morison was prosecuted cover a different kind of offense than that of "spying," and that, pursuant to these sections, the Act properly extends to disclosure of classified material to any person "not entitled to receive" it.⁶⁴

By the same token, however, two of the three judges who voted to affirm Morison's conviction went out of their way to distinguish Morison from the press. The Court as a whole pointed out that, as a government intelligence employee, Morison expressly had been placed on notice of his obligations under the Act in his written employment agreement and was being prosecuted for "purloining" obviously classified military documents and transmitting them to a person not entitled to receive them, in direct violation of the legal obligations to which he had subscribed by accepting employment.⁶⁵ Judge Wilkinson wrote separately to explain that, "Morison as a source would raise newsgathering rights on behalf of press organizations that are not being, and probably could not be, prosecuted under the espionage statute," and observed that "it is important to emphasize what is *not* before us today. This prosecution was not an attempt to apply the espionage statute to the press for either the receipt or publication of classified materials."⁶⁶

62 844 F.2d 1057 (4th Cir. 1988).

63 *Id.* at 1060-61, 1076-77.

64 *Id.* at 1065.

65 *Id.* at 1068.

66 *Id.* at 1081, 1085 (Wilkinson, J., concurring); *see also id.* at 1086 (Phillips, J., concurring) (observing that Morison's conviction should not be construed to "threaten[] the vital newsgathering functions of the press").

C. The Espionage Act and the Press

While the Sedition Act of 1798 was invoked almost exclusively against members of the press (and arguably was enacted precisely for that purpose), the paucity of prosecutions against journalists under the Espionage Act reflects a hesitation on the part of the Executive to deploy its firepower against the press, a hesitation likely explained at least in part by the separate judicial developments concerning the First Amendment during the century-long interval between the two legislative enactments.⁶⁷

The only known invocation of the Espionage Act directly against the press arose not in a criminal prosecution, but in the context of a failed attempt by the Nixon Administration to obtain an injunction to prevent publication of what are now known as the Pentagon Papers—a “leak” that remains one of the most significant disclosures of classified material in American history. As is by now well known, in 1971, *The New York Times* and the *Washington Post* began publishing portions of approximately 7,000 pages of classified documents relating to Vietnam policy, leaked by defense analyst Daniel Ellsberg. The documents revealed a startling disconnect between the public statements of members of the Johnson and Kennedy Administrations and their private doubts regarding a successful conclusion of the war.⁶⁸ When the government filed suit seeking an injunction against publication of the documents, it relied not only on its inherent power to protect national defense, but also invoked as statutory authority for injunctive relief section 793(e) of the Espionage Act, which makes it unlawful for anyone who has “unauthorized possession of” documents “relating to the national defense” with “reason to believe [the information] could be used to the injury of the United States or to the advantage of a[] foreign nation” to “willfully communicate” the information to persons not entitled to receive it. In other words, the government asserted that section 793(e) barred publication (*i.e.*, willful communication) of the material at issue. An injunction was necessary to prevent the commission of a crime—a crime that would have a serious, negative impact on national security, according to the Attorney General. When *New York Times Co. v. United States*⁶⁹ reached the Supreme Court, therefore, the question was not whether the newspaper could be criminally prosecuted under the Espionage Act but, rather, whether the government was entitled to the extraordinary relief of a prior restraint on publication of newsworthy information in the name of “national security.” The Court, in a very brief, per curiam order, ruled that the government had not met its burden of showing that it was entitled to such pre-publication injunctive relief.

67 Indeed, except where a journalist has affirmatively engaged in an unlawful physical act, such as trespass or the removal of evidence from the scene of an investigation, *see, e.g., United States v. Sanders*, 17 F. Supp. 2d 141 (E.D.N.Y. 1998), *aff'd*, 211 F.3d 711 (2d Cir. 2000), it does not appear that other criminal statutes have been invoked successfully to prosecute newsgatherers in analogous contexts. In 1973, an investigative reporter in Washington, D.C. was charged as a principal under 18 U.S.C. § 641 with receiving stolen government documents, but the charges were dropped when the grand jury later refused to indict him. *See* Mark Feldstein, *The Jailing of a Journalist: Prosecuting the Press for Receiving Stolen Documents*, 10 COMM. L. & POLICY 137, 161 (2005).

68 It is worth noting that the complete set of the Pentagon Papers have since been declassified and released, as of June 13, 2011, some 40 years after the newspapers began publishing them. *See Pentagon Papers Released 40 Years After New York Times Began Publishing Them* (June 13, 2011, 9:18 pm ET), <http://huff.to/mr4n1O>.

69 403 U.S. 713 (1971).

Sharp doctrinal disagreement among the justices was reflected in the multiple concurring and dissenting opinions. Justice Black, writing in concurrence, put the matter most strongly:

Madison and the other Framers of the First Amendment, able men that they were, wrote in language they earnestly believed could never be misunderstood: “Congress shall make no law abridging the freedom . . . of the press . . .” 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.⁷⁰

Of the six Justices concurring in the result, three -- Stewart, White and Marshall -- pointed out (albeit in dicta) the possibility that the newspaper could be prosecuted after-the-fact. Indeed, Justice White arguably invited the government to pursue some form of post-publication prosecution against *The Times*, observing that “failure by the Government to justify prior restraints does not measure its constitutional entitlement to a conviction for criminal publication. That the Government mistakenly chose to proceed by injunction does not mean that it could not successfully proceed in another way. . . . I would have no difficulty in sustaining convictions under these sections on facts that would not justify the intervention of equity and the imposition of a prior restraint.”⁷¹ As no attempt to prosecute the newspaper followed, the courts were never called upon to resolve the question of whether the Espionage Act could be applied to the press in this circumstance.

D. Assange and the Espionage Act

Since the November 2010 leak of diplomatic cables, pressure in the U.S. to prosecute Assange or WikiLeaks has been building. Immediately after the release, White House press secretary Robert Gibbs stated, “I think it is safe to say that [President Obama] was—it’s an understatement—not pleased with this information becoming public. . . [O]pen and transparent government is something that the President believes is truly important. But the stealing of classified information and its dissemination is a crime.”⁷² The White House further called the release of the “stolen cables” to various newspapers a “reckless and dangerous action” and warned that the full release of some cables could hamper joint American-foreign operations and risk the work and lives of the confidential sources of American diplomats.⁷³ The threat of

⁷⁰ *Id.* at 716-17 (Black, J., concurring).

⁷¹ *Id.* at 733-37 (White, J., concurring).

⁷² “Press Briefing by Press Secretary Robert Gibbs, 11/29/2010,” [White House Office of the Press Secretary](http://1.usa.gov/e5QELh), <http://1.usa.gov/e5QELh>.

⁷³ Andrew Lehren & Scott Shane, *Leaked Cables Offer Raw Look at U.S. Diplomacy*, N.Y. TIMES (Nov. 28, 2010), <http://nyti.ms/hfy0Rk>.

further publication of diplomatic cables also prompted massive reviews of documents at U.S. embassies around the world.⁷⁴

Congressional leaders—both Republican and Democrat—condemned the leak as reckless. Connecticut Senator Joe Lieberman, former chairman of the Senate Homeland Security and Governmental Affairs Committee, called the leak ““nothing less than an attack on the national security of the United States.””⁷⁵ Lieberman added:

“By disseminating these materials, WikiLeaks is putting at risk the lives and the freedom of countless Americans and non-Americans around the world. It is an outrageous, reckless, and despicable action that will undermine the ability of our government and our partners to keep our people safe and to work together to defend our vital interests. Let there be no doubt: the individuals responsible are going to have blood on their hands.”⁷⁶

Current chairman of the House Homeland Security Committee, New York Representative Peter King, even urged that WikiLeaks be deemed a “terrorist organization” and asked U.S. Attorney General Eric Holder to charge Assange under the Espionage Act for conspiracy to disclose classified information.⁷⁷ In December 2010, the House Judiciary Committee held a hearing to address WikiLeaks. Testimony focused primarily on whether the Espionage Act should be revised to make it easier to prosecute recipients of classified information.

At about the same time, reports surfaced that a grand jury had been convened in Alexandria, Virginia (home to the Pentagon) to investigate WikiLeaks and Assange. Assange’s original attorney in connection with efforts to extradite him to Sweden on sex-crimes charges, Mark Stephens, told the Al-Jazeera network in a December interview, “[w]e have heard from Swedish authorities there has been a secretly empanelled grand jury in Alexandria. . . . They are currently investigating this.”⁷⁸ Efforts by Twitter to gain permission from the court in Virginia to disclose to its customers the existence of secret demands from the government (akin to a pre-litigation subpoena) for information concerning those customers’ accounts provided a further public glimpse of the grand jury’s investigation. The no-longer secret demands concerned,

74 Jill Dougherty, *WikiLeaks threat sparks massive review of diplomatic documents*, CNN.COM (Nov. 25, 2010), <http://bit.ly/ghwaBe>.

75 Stephanie Condon, *Congress Lashes Out at Wikileaks, Senators Say Leakers May Have "Blood on their Hands"*, CBS NEWS (Nov. 29, 2010, 5:00 pm ET), <http://bit.ly/qhyi5R>.

76 *Id.*

77 *Id.*

78 *Assange attorney: Secrete grand jury meeting in Virginia on WikiLeaks*, CNN.COM (Dec. 13, 2010), <http://bit.ly/ebLrAr>.

among others, an Icelandic legislator who has been a strong supporter of Assange.⁷⁹ And, on April 26, 2011, the Federal Bureau of Investigation served a subpoena in Boston, Massachusetts on a Cambridge resident, compelling his appearance to testify in Virginia. That same month, Assange asserted during an appearance via Skype at a journalism conference in Berkeley, California, that the grand jury was targeting a group of students and activists in Boston for assisting Manning with respect to the classified diplomatic cables.⁸⁰ The subpoena to the Boston resident states that the grand jury is investigating parties for “‘knowingly accessing a computer without authorization,” something Manning has been directly accused of doing to obtain the secret cables.⁸¹ The subpoena, however, also references the generic federal criminal conspiracy statute, which makes it a crime to “conspire to commit any offense” or to “defraud” the United States,⁸² as well as the conspiracy provision of the Espionage Act, which imposes criminal liability on those who “conspire to violate” other provisions of the Act.⁸³

As of this writing, only Manning has actually been charged with the leaks in question. The service of the subpoena, the government’s continued reliance on the Espionage Act, and its pursuit of social media account information belonging to avowed supporters of Assange, however, suggest that the investigation into Assange and WikiLeaks continues. But how would the government proceed with such a prosecution? Setting aside the question of extradition (and also the question of whether Assange, a non-citizen, would be entitled to the same substantive legal rights as a U.S. citizen), in order to convict Assange under the Act, the government would have to demonstrate that Assange was an “unauthorized” possessor of a protected document, and that, while having “reason to believe [it] could be used to the injury of the United States or to the advantage of any foreign nation,” Assange communicated or transmitted the document “to any person not entitled to receive it.”⁸⁴ The government’s burden to prove “bad intent” has been perceived as the stumbling block to prosecution of journalists in the past, but, in the view of at least one commentator, if the publisher acted with the requisite intent, the Act would appear to afford a basis on which to prosecute someone in Assange’s position.⁸⁵

Whether section 793(e) of the Espionage Act properly could be applied to the press was first discussed generally by the New York trial court in the Pentagon Papers case. In his opinion, Judge Gurfein suggested that the statutory language itself, along with certain legislative history

79 See, e.g., Dominic Rushe, *Icelandic MP fights US demand for her Twitter account details*, THE GUARDIAN (Jan. 8, 2011), <http://bit.ly/g18KFT>.

80 Michael Riley, *WikiLeaks Grand Jury Witness Says He Declined to Answer Queries on Manning*, BLOOMBERG (June 15, 2011, 7:00 pm), <http://bloom.bg/jNWtLN>.

81 Glenn Greenwald, *FBI serves Grand Jury subpoena likely relating to WikiLeaks*, SALON (Apr. 27, 2011, 13:28 ET), <http://bit.ly/jj9JPR>.

82 18 U.S.C. § 371.

83 18 U.S.C. § 793(g); see also Greenwald, *supra* note 82.

84 18 U.S.C. § 793(e).

85 See Geoffrey R. Stone, *Government Secrecy vs. Freedom of the Press*, 1 HARV. L. & POL’Y REV. 185, 217 (2007).

indicated “that newspapers were not intended by Congress to come within the purview of Section 793.”⁸⁶ Yet, as noted above, while declining to enjoin publication of the Pentagon Papers, several justices of the Supreme Court did not rule out government prosecution of the newspapers under the Espionage Act.

Perhaps the closest parallel to WikiLeaks in recent years arose when two employees of the lobbying group American Israel Public Affairs Committee (“AIPAC”) were charged—in the same courthouse in Virginia in which a grand jury apparently is now investigating Assange—with violating the Espionage Act. They were not government employees themselves; rather, they obtained sensitive information through a leak from a Defense Department employee and then transmitted or sought to transmit that information to others. Steven J. Rosen served for 23 years as one of the top officials of AIPAC, while Keith Weissman served for years as a senior Iran analyst with AIPAC. The two men were charged under sections 793(d) (persons with unauthorized possession of national defense information who transmit it to unauthorized recipients) and 793(g) (conspiracy) of the Espionage Act in a convoluted case that began in 2005. Had the case proceeded to trial, it would have been the first prosecution under the Espionage Act in which essentially no documents were involved. In every other prosecution to date, defendants have transferred tangible items, such as documents or photographs, to a foreign government or its agent. Here, with one exception, the information was transmitted orally.

The indictment against Rosen and Weissman charged that they conspired to obtain classified information from government officials in order to relay it to other lobbyists, journalists and diplomats, including representatives of Israel. Some of the information pertained to Iranian operations against U.S. forces in Iraq. Lawrence Franklin, an official working in Defense Secretary Donald Rumsfeld’s office, passed the information to Rosen and Weissman. Franklin pled guilty to, among other charges, communicating and conspiring to communicate national defense information to people not entitled to receive it under the same sections of the Act (sections 793(d) and (g)) invoked against Rosen and Weissman.⁸⁷ Franklin was sentenced in January 2006 to just over twelve years in prison and a \$10,000 fine. His sentence later was reduced to ten months house arrest for his cooperation in the Rosen and Weissman cases.⁸⁸

To the surprise of many observers, following Franklin’s plea, the government nevertheless proceeded against Rosen and Weissman for re-transferring to members of the press and others the allegedly classified information they had received from Franklin. In response, the defendants moved to dismiss the indictment on several grounds, including that the statute’s reference to “information relating to the national defense” was unconstitutionally vague, and that the statute impermissibly infringed their own First Amendment rights and would chill the First Amendment rights of others because of uncertainty over what discussion of national security issues is prohibited. Numerous amici curiae filed briefs urging the trial court to dismiss the charges on free speech grounds.

86 *United States v. New York Times Co.*, 328 F. Supp. 324, 329 (S.D.N.Y. 1971) (subsequent history omitted).

87 *United States v. Rosen*, 599 F. Supp. 2d 690, 693 n.4 (E.D. Va. 2009).

88 Jerry Markon, *Sentence Reduced In Pentagon Case*, WASH. POST, June 12, 2009, at A12.

In a 2006 opinion, U.S. District Court Judge T.S. Ellis denied the motion to dismiss the indictment, holding the Espionage Act constitutional on its face and as applied to Rosen and Weissman. Judge Ellis did, however, reject the government’s threshold argument that no First Amendment issue is presented by such an indictment. Citing *Morison*, Judge Ellis emphasized that “the mere invocation of ‘national security’ or ‘government secrecy’ does not foreclose a First Amendment inquiry. Rather, the character of every act depends on the circumstances in which it was done.”⁸⁹ Nevertheless, in the case of the Espionage Act, Judge Ellis identified the reasons why, when construed properly, he held the Act to be consistent with the Constitution.

First, relying on *Gorin*, *Morison* and other earlier cases, Judge Ellis observed that the term “information related to the national defense” was limited to information “closely held” by the government.⁹⁰ Second, according to Judge Ellis, earlier cases established that the Act applies only to information of a type the disclosure of which “would be potentially damaging to the United States or useful to an enemy of the United States.”⁹¹ Third, earlier case law also established that conviction under the Act requires the government to prove that the defendant “willfully” violated its terms—that is, acted with the specific intent to violate the statute.⁹² Finally, where a prosecution rests on the catch-all phrase “other information related to the national defense” and involves intangible information (rather than for example, the dissemination of specific tangible documents such as a diagram of a military base or a weapon), Judge Ellis held that the Act further requires the government to prove that the defendant, in disclosing the information, subjectively intended “to either harm the United States or to aid a foreign government.”⁹³ Clearly, for those members of the press who trade in intangible information, rather than tangible materials, this is of some significance.

Taken together, Judge Ellis concluded, these limitations on the reach of the Espionage Act as applied to a civilian recipient of national defense information in intangible form reflect an appropriately narrow and effective approach by the government to protect an interest of the highest order, *i.e.*, the security of the nation, such that the Act is consistent with the First Amendment.⁹⁴ In short, while “rejecting” the defendants’ First Amendment challenge to the Espionage Act, in construing the Act so as to be consistent with the First Amendment, Judge Ellis articulated an imposing burden for the government: It would have to prove that Rosen and Weissman, intending to violate the Act, disseminated what they knew to be secret information, that the information objectively was of a kind that could injure the U.S., and that Rosen and Weismann subjectively knew of its potential to harm the U.S. when they disclosed it. Although it took almost three years from the date of this ruling, it did not come as a great surprise when, on

⁸⁹ *United States v. Rosen*, 445 F. Supp. 2d 602, 632 (E.D. Va. 2006) (citation omitted), *aff’d on other grounds*, 557 F.3d 192 (4th Cir. 2009).

⁹⁰ *Id.* at 620-21.

⁹¹ *Id.* at 621 (quoting *Morison*, 844 F.2d at 1071-72).

⁹² *Id.* at 625 & n.30.

⁹³ *Id.* at 625-26.

⁹⁴ *Id.* at 640-41 & 643.

May 1, 2009, prosecutors announced they would ask Judge Ellis to dismiss the charges against Rosen and Weissman because of “the diminished likelihood the government will prevail at trial under the additional intent requirements imposed by the court and the inevitable disclosure of classified information that would occur at any trial.”⁹⁵

Would the same obstacles to prosecution of Rosen and Weissman arise were the government to obtain an indictment of Assange?

1. The problem of proving willfulness

As noted, section 793(e) of the Espionage Act prohibits the willful communication to “any person not entitled to receive it,” of “any document” or “information relating to national defense” which “the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation.” By his own admissions in the public record, it seems clear that Assange intended to and did disseminate to people not entitled to receive or possess them, tangible documents related to the national defense, and that at least some of these documents were both secret and objectively of a kind the disclosure of which had the potential to harm the security of the United States, and that Assange was aware of the secret nature of the documents. If that is correct, and if whichever judge were assigned to the case adhered to Judge Ellis’ articulation of the government’s burden under the Act with regard to a civilian recipient of such information (recall that the Assange grand jury is meeting in the same courthouse where Judge Ellis sits), then the only remaining question is whether the government can demonstrate that Assange knew that disclosure of the documents “was illegal, but proceeded nonetheless”—that is, that he acted “with ‘a bad purpose either to disobey or to disregard the law.’”⁹⁶

A mainstream news organization in the United States that released the same documents as WikiLeaks doubtless would answer this charge by declaring that its intent was to inform the public of matters pertinent to self-government, not to violate the statute or to injure the government—a characterization of intent that courts have accepted in analogous circumstances.⁹⁷

⁹⁵ Kathleen Cullinan, *Charges to be Dropped in AIPAC case*, THE REPORTERS COMMITTEE FOR FREEDOM OF THE PRESS (May 1, 2009, 5:02 pm), <http://bit.ly/qJdXPJ>. Before dropping the case, the government took an interlocutory appeal to the Fourth Circuit challenging the district court’s ruling that would have allowed the defendants to disclose at trial numerous classified documents, an appeal the Fourth Circuit denied. 557 F.3d 192, 200 (4th Cir. 2009). In so holding, the court also noted that “the government’s attempt to piggyback a pretrial review of the [trial] court’s interpretation of § 793 is improper at this juncture,” and it refused to consider the correctness of the burden set out by Judge Ellis. *Id.* at 199.

⁹⁶ *Rosen*, 445 F. Supp. 2d at 625, 643. Because Assange, unlike Rosen and Weissman, is not dealing exclusively in “intangible information,” Judge Ellis’ additional requirement that the government prove subjective awareness of the potentially harmful nature of the information would not seem to be implicated. Of course, if there were evidence that Assange had entered into a conspiracy with Manning to obtain the information, liability could be founded on the conspiracy provision alone.

⁹⁷ For example, generally the tort of intentional infliction of emotional distress requires a plaintiff to prove that the defendant acted intentionally or recklessly and that the natural and probable consequences of the action would cause

With specific reference to WikiLeaks' release of the diplomatic cables, Baruch Weiss, one of the attorneys on the defense team for Weissman and Rosen, notes that "well before publishing the cables, [Assange] wrote a letter to the U.S. government, delivered to our ambassador in London, inviting suggestions for redactions. The State Department refused. Assange then wrote another letter to State, reiterating that "WikiLeaks has absolutely no desire to put individual persons at significant risk of harm, nor do we wish to harm the national security of the United States."⁹⁸

More generally, WikiLeaks affirmatively characterizes itself in terms familiar to mainstream media: Prominently displayed on its home page is a quotation from *Time* magazine, "Could become as important a journalistic tool as the Freedom of Information Act," followed by its self-description as "a non-profit media organization dedicated to bringing important news and information to the public." WikiLeaks describes its writers as "journalists," emphasizes that it does not solicit leaks of classified or otherwise private materials (but also includes an anonymous, digital drop-box for delivery of secret materials to it), asserts that it vets leaked materials for authenticity, and describes itself as providing analysis of leaked documents with links to the documents themselves so that readers may verify its analysis.⁹⁹

More specifically, in connection with each cache of original, leaked material, WikiLeaks provides introductory notes—some brief, some more elaborate—providing context for and a guide to understanding the underlying source materials. If often more akin to an "abstract" or "press release" than a news article, the notes are expressive matter that serves the purpose, at a minimum, of orienting a reader to, and often summarizing at a high level the underlying documents.¹⁰⁰ Yet no countervailing views are offered and, as some note, the accounts fail to distinguish between opinion and fact.¹⁰¹ As for the documents themselves, WikiLeaks generally engages in no selection or editing of them, although some larger caches are organized into categories or otherwise indexed to help readers locate specific information within the documents. Many of the caches of documents are accompanied by what would, on a mainstream news organization's website, be classified as an "editorial." For instance, in the course of a multi-page introduction describing the Guantanamo Bay prisoner files released in April 2011, WikiLeaks observes:

the plaintiff emotional distress. Courts have squarely held that intentional publication of a news report does not amount to intent to inflict harm. *E.g.*, *Levin v. McPhee*, 917 F. Supp. 230 (S.D.N.Y. 1996) (no evidence defendants' conduct directly targeted plaintiff; cause of action dismissed), *aff'd* 119 F.3d 189 (2d Cir. 1997); *Witherspoon v. Phillip Morris Inc.*, 964 F. Supp. 455, 463 (D.D.C. 1997) (holding that intent to cause harm must be specifically directed toward the person complaining of such harm, rather than toward the public at large).

98 Baruch Weiss, *Why prosecuting WikiLeaks' Julian Assange won't be easy*, WASH. POST (Dec. 5, 2010), <http://wapo.st/gyuVpP>.

99 See generally <http://wikileaks.org>.

100 See, e.g., *Secret US Embassy Cables*, WIKILEAKS, <http://wikileaks.org/cablegate.html>.

101 Jonathan Peters, *WikiLeaks Would Not Qualify to Claim Federal Reporter's Privilege in Any Form*, 63 FED. COMM. L.J. 667, 681 (2011).

Uncomfortable facts like these are not revealed in the deliberations of the Joint Task Force, but they are crucial to understanding why what can appear to be a collection of documents confirming the government's scaremongering rhetoric about Guantánamo—the same rhetoric that has paralyzed President Obama, and revived the politics of fear in Congress—is actually the opposite: the anatomy of a colossal crime perpetrated by the US government on 779 prisoners who, for the most part, are not and never have been the terrorists the government would like us to believe they are.¹⁰²

WikiLeaks embraces what it describes as a non-traditional news medium and “a new model of journalism,”¹⁰³ something akin to “scientific journalism.” Similar to a wire service, the site claims, “WikiLeaks reports stories that are often picked up by other media outlets. We encourage this. We believe the world’s media should work together as much as possible to bring stories to a broad international readership.”¹⁰⁴ It cites the Pentagon Papers case, and proclaims its agreement with the court’s holding that “only a free and unrestrained press can effectively expose deception in government.”¹⁰⁵ Indeed, with regard to the April 2010 release of the “Collateral Murder” videotape, it would be difficult to argue that WikiLeaks performed no traditional journalistic functions: Not only did WikiLeaks edit and caption the video, it apparently sent personnel to Iraq to interview Iraqi witnesses about the incident, and provided both reports of these interviews and an “eye witness” account from a U.S. soldier.¹⁰⁶ The release of the video, which Reuters had unsuccessfully sought for years, was widely covered by news organizations in the United States and abroad.¹⁰⁷

These facts notwithstanding, some commentators have resisted classifying WikiLeaks as a news organization. Typically, such commentators cite WikiLeaks’ heavy focus on the posting of (largely) unmediated source material, the lack of transparency in its vetting process, and the lack of accountability attributable to its secretive editorial and organizational existence. Lucy Dalglish, executive director of the Reporters Committee for Freedom of the Press, has pointed out that Assange “has done some things that journalists do, but I would argue that what the *New York Times* does is more journalism. They vet the information . . . They consider outside sources. They take responsibility. They publicly identify themselves. . . . They do some value

102 Andy Worthington, *WikiLeaks Reveals Secret Files on All Guantanamo Prisoners*, WIKILEAKS, <http://wikileaks.ch/gitmo/>.

103 *What is WikiLeaks?*, WIKILEAKS, <http://wikileaks.org/About.html>.

104 *Id.*

105 *About*, WIKILEAKS, <http://www.wikileaks.org/About.html>.

106 *See Collateral Murder*, WIKILEAKS (Apr. 5, 2010, 10:44 EST), <http://www.collateralmurder.com/>.

107 *See, e.g.*, Joby Warrick, *Exposing secrets through secrecy; Cloaked in the virtual world, WikiLeaks gives whistleblowers a powerful platform*, WASH. POST, May 20, 2010, at A01; *Collateral Murder Video Exposes the Fallacy of National Security*, DIGITAL JOURNAL, April 14, 2010; Noam Cohen & Brian Stelter, *Airstrike Video Brings Attention to Whistle-Blower Site*, N.Y. TIMES, April 7, 2010 at A8.

added. They do something original to it.”¹⁰⁸ Jonathan Peters, a lawyer and research fellow at the Missouri School of Journalism, has offered a similar view:

Although [the WikiLeaks process] may look a little like journalism, investigative or otherwise, it is no such thing. WikiLeaks does not engage in multi-article reporting. It does not do extensive interviewing for its news stories. It does not provide meaningful context or journalistic analysis. It does not, in short, “make an understandable story out of the mountain of information” it has gathered.¹⁰⁹

Among the specific criticisms leveled at Assange is a failure on his part to acknowledge that a news publisher sometimes has an obligation to *withhold* information in service of the public interest. For example, as reported in a PBS broadcast titled “WikiSecrets” that examined, among other things, WikiLeaks’ release of the diplomatic cables purportedly received from Bradley Manning, Assange is quoted as saying that the site was careful to employ a “harm-minimization process” that included redacting details that might have endangered lives. The PBS report, however, cited “insiders within the organization” as accusing Assange of only considering redactions as an afterthought and performing them hastily before publication.¹¹⁰ When WikiLeaks published the Afghanistan documents in July 2010, it withheld some 15,000 that it said were especially sensitive, but did not remove the names of Afghan intelligence sources from some of the published documents.¹¹¹ Assange’s “former-right-hand man” and WikiLeaks spokesperson Daniel Domscheit-Berg has publicly claimed that Assange acted negligently in this regard.¹¹² Significantly, considering the primary obstacle to invoking the Espionage Act against the press, one journalist who worked with Assange has alleged that he expressly wished harm on U.S. allies:

Was Julian Assange prepared to publish some of the leaked documents without adequately redacting the names of people who could have been harmed by the disclosures? “Julian was very reluctant to delete those names, to redact them.” David Leigh of the Guardian newspaper tells FRONTLINE of meetings he attended with Assange in the run-up to publication of the war logs. “And we said: ‘Julian, we’ve got to do something about these redactions. We really have got to.’ And he said:

108 Nancy A. Youssef, *In WikiLeaks fight, U.S. journalists take a pass*, McClatchy (Jan. 9, 2011), <http://bit.ly/g7MZox>.

109 Peters, *supra* note 102 at 680.

110 *Introduction*, PBS FRONTLINE WIKISECRETS (May 24, 2011), <http://to.pbs.org/itvaMf>.

111 Peters, *supra* note 102, at 684.

112 *Interview: Daniel Domscheit-Berg*, PBS FRONTLINE WIKISECRETS (May 24, 2011), <http://to.pbs.org/jFbfWI>.

‘These people were collaborators, informants. They deserve to die.’
And a silence fell around the table.”¹¹³

U.S. Defense Secretary Robert Gates similarly has accused Assange of putting lives at risk, and Joint Chiefs of Staff Chair Admiral Mike Mullen suggested that WikiLeaks “‘might already have on their hands the blood of some young soldier or that of an Afghan family.’”¹¹⁴

Others have taken a somewhat different view. As Professor Stephen L. Carter notes:

What Assange has done is little different from a person who illegally obtains the tax returns of leading journalists, and posts them online, showing how much money each earns, and from whom, and where each gives it away, all in order, he might say, to demonstrate their biases. Such an individual is worthy of condemnation, not celebration. But acting callously, or self-interestedly, or narcissistically, ought not to be criminal, particularly when what is involved is, undeniably, speech.¹¹⁵

Indeed, apart from the question of whether Assange, or WikiLeaks as an organization, could be said to have acted with the intent to violate the Espionage Act and thereby to harm the U.S. or benefit its enemies, it is difficult to discern a compelling argument that any of the other factual distinctions between WikiLeaks and “mainstream news organizations” matter when it comes to seeking shelter under the First Amendment. Properly understood, at least according to one observer, the First Amendment “doesn’t much care whether WikiLeaks is a reputable news outlet, a gang of black-hat hackers, or a traveling circus,” precisely because the protections it affords “depend on what WikiLeaks publishes, not what it is.”¹¹⁶ Indeed, it is well accepted that “[t]he press in its historic connotation comprehends every sort of publication which affords a vehicle of information and opinion.”¹¹⁷ As Bill Keller, executive editor of *The New York Times*, has acknowledged:

“It’s very hard to conceive of a prosecution of Julian Assange that wouldn’t stretch the law in a way that would be applicable to us,” said Keller. “Whatever one thinks of Julian Assange, certainly American

113 *Introduction*, *supra* note 111.

114 Peters, *supra* note 102, at 684 (quoting Noam Cohen, *A Renegade Site, Now Working with the News Media*, N.Y. TIMES, Aug. 2, 2010, at B3).

115 Stephen L. Carter, *The Espionage Case Against Assange*, The Daily Beast (Dec. 1, 2010, 6:26 pm EST), <http://bit.ly/qUKGQV>.

116 Andy Greenberg, *Is WikiLeaks a Media Organization? The First Amendment Doesn’t Care*, FORBES (Apr. 21, 2011, 9:57 am), <http://onforb.es/hH4Of5>.

117 *Lovell v. City of Griffin*, 303 U.S. 444, 452 (1938).

journalists, and other journalists, should feel a sense of alarm at any legal action that tends to punish Assange for doing essentially what journalists do. That is to say, any use of the law to criminalize the publication of secrets.”¹¹⁸

If there is a meaningful distinction to be drawn between WikiLeaks and the traditional press for purposes of application of the Espionage Act, it may well be only the specific intent of the publisher with regard to the criminal statute in question.

2. The *Daily Mail/Florida Star/Bartnicki* principle

Beyond the requirement that the government prove the requisite intent in order to secure a conviction under the Espionage Act, however, there remains the question of whether application of its proscriptions to WikiLeaks would be constitutional in the circumstances of the particular disclosures. As noted, the courts have never been directly confronted with the prosecution of a press-like organization or an individual journalist under the statute, at least not in the era of modern First Amendment jurisprudence.

As colleagues of ours have put it in a recent law review article, “[c]ontemporary interpretation of the First Amendment proceeds from the premise that “[t]he freedom of speech and of the press guaranteed by the Constitution embraces at the least the liberty to discuss publicly and truthfully all matters of public concern without . . . fear of subsequent punishment.”¹¹⁹ In a series of cases beginning with *Smith v. Daily Mail* in 1979, the Supreme Court repeatedly has underscored that “truthful information about a matter of public concern” receives very broad protection from criminal or civil liability.¹²⁰ Often referred to as “the *Daily Mail* principle,” this bedrock constitutional requirement was most recently explicated by the Supreme Court in *Bartnicki v. Vopper*, a case arising under the federal Wiretapping Act, which criminalizes and creates a civil remedy for the unlawful interception and dissemination of wire and wireless communications.¹²¹ Where truthful information about a matter of public

118 Sam Gustin, *Times Editor Alarmed by Prospect of WikiLeaks Prosecution*, WIRED (Feb. 3, 2011, 10:24 PM), <http://bit.ly/gTHy6D>.

119 Lee Levine, Nathan E. Siegel and Jeanette Melendez Bead, *Handcuffing the Press: First Amendment Limitations on the Reach of Criminal Statutes as Applied to the Media*, 55 N.Y.L. SCH. L. REV. 1015, 1017 (2011) (quoting *Thornhill v. Alabama*, 310 U.S. 88, 101-02 (1940)).

120 *Smith v. Daily Mail*, 443 U.S. 97, 103 (1979) (in context of claim that newspaper published name of juvenile assailant in violation of state law, holding that “if a newspaper lawfully obtains truthful information about a matter of public significance then state officials may not constitutionally punish publication of the information, absent a need to further a state interest of the highest order.”); *Florida Star v. B.J.F.*, 491 U.S. 524, 533-34 (1989) (same with regard to publication of name of rape victim in violation of state law); see also *Garrison v. Louisiana*, 379 U.S. 64, 74 (1964) (“[t]ruth may not be the subject of either civil or criminal sanctions”); *Snyder v. Phelps*, 131 S. Ct. 1207 (2011) (in context of protecting offensive protests at military funerals, observing that, “[a]s a Nation we have chosen . . . to protect even hurtful speech on public issues to ensure that we do not stifle public debate”).

121 532 U.S. 514 (2001).

significance is at issue, the Court reaffirmed, “then state officials may not constitutionally punish publication of the information, absent a need . . . of the highest order.”¹²²

Of significance to Assange, the Supreme Court also has emphasized that the degree of protection afforded by the First Amendment in this regard does not vary based upon the identity of the speaker or the perceived social utility of the information disseminated.¹²³ Furthermore, in *Bartnicki*, with reference to the circumstance in which the publisher obtains the information lawfully but knows the source of it has acted unlawfully in procuring or disseminating it, the Court squarely held that “a stranger’s illegal conduct does not suffice to remove the First Amendment shield from speech about a matter of public concern.”¹²⁴ Significantly, this shield is breached, the Court has said, when the publisher goes beyond knowing acceptance of material obtained unlawfully by another to actual participation in illegally obtaining the material.¹²⁵ This no doubt explains the disclaimers now on WikiLeaks’ own website and on sites of those organizations that have launched similar models that expressly disavow any desire to induce (and in some cases, disavow willingness to accept the fruit of) unlawful disclosures by the source.

Perhaps the closest analogy to WikiLeaks in these regards is presented by *Jean v. Mass. State Police*.¹²⁶ There, Mary T. Jean posted to the Internet an audio and video recording of an arrest and warrantless residential search despite her knowledge at the time that the recording given to her had been made illegally.¹²⁷ Applying *Bartnicki*, the U.S. Court of Appeals for the First Circuit held that the First Amendment protected Jean from criminal liability. The court held that the government’s interest in protecting private communication, which was “clearly implicated” in *Bartnicki*, was “virtually irrelevant” in Jean’s case because the intercepted communications involved “a search by police officers of a private citizen’s home in front of that individual, his wife, other members of the family, and at least eight law enforcement officers.”¹²⁸ The court also held that the state’s interest in punishing a subsequent publisher of information was entitled to even less weight in Jean’s case, where the identity of the interceptor was known, and presumably could be charged and, if convicted, punished.¹²⁹ Additionally, the court determined that there was no distinction between Jean’s “active collaboration” in the chain of dissemination as opposed to the “passive” conduct in *Bartnicki*. In both cases, the court held,

122 *Id.* at 527-28.

123 See Levine, et al. *supra* note 120, at 1019 nn.23-24 (citing *Lovell v. City of Griffin*, 303 U.S. 444, 452 (1938); *Schad v. Borough of Mt. Ephraim*, 452 U.S. 61, 65 (1981); *Mills v. Alabama*, 384 U.S. 214, 219 (1966); *Hustler Magazine v. Falwell*, 485 U.S. 46, 48 (1988)).

124 *Bartnicki*, 532 U.S. at 517-18, 528, 535.

125 *Id.* at 525, 527-28, 532 n.19 (quoting *Branzburg v. Hayes*, 408 U.S. 665, 691 (1972)).

126 492 F.3d 24 (1st Cir. 2007).

127 *Id.* at 31; see also Levine, et al. *supra* note 120, at 1026.

128 *Jean*, 429 F.3d at 30.

129 *Id.*

there was a decision to proceed with the disclosures even though the tapes were illegally obtained.¹³⁰ Both knowing disclosures were protected by the First Amendment.¹³¹

Assuming that, in Assange's case, he did not in fact act in concert with WikiLeaks' sources in their presumptively illegal initial acts of acquisition and disclosure sufficiently to vitiate application of the *Daily Mail* principle in the first instance (*i.e.*, Assange himself acted lawfully by merely receiving the leaked materials), and assuming that the government could otherwise meet its burden of proof, would the government be able successfully to demonstrate that application of the Espionage Act to Assange legitimately serves an interest of "the highest order"? Protection of the national security, including the secrets necessary to that security, seems plainly to qualify as a national interest of the highest order.¹³² The more precise question would be whether the contents of the leaked documents published by WikiLeaks reflect such interests. For example, one commentator has argued that, if the cables disclosed the names of secret agents in Afghanistan or Iraq, outlined future war plans, or contained something of similar practical harm, the standard might be met.¹³³

III. WHAT IF THE LEAKED CABLES BELONGED TO THE BRITISH GOVERNMENT?

Given the origins of the Espionage Act in part in the British Official Secrets Act ("OSA"), a brief comparison of the former to the current version of the latter is interesting in its own right, as well as illustrative of the impact of the First Amendment on such legislation. The OSA (there are actually two separate Acts currently in effect) is intended to protect certain official information relating to security and intelligence from disclosure. Dating back to 1889, the U.K.'s OSA criminalizes the sharing, disclosure, or publication of government information by employees and former employees of the intelligence and security forces, as well as the disclosure of such information by others, including journalists. Specifically, the principal operative sections of the OSA provide:

A person who is or has been—

(a) a member of the security and intelligence services; or

(b) a person notified that he is subject to the provisions of this subsection,

¹³⁰ *Id.* at 32.

¹³¹ *Id.*

¹³² *E.g.*, *Rosen*, 445 F. Supp. 2d at 633-34 (citing cases).

¹³³ See Andy Sellars, *WikiLeaks and the First Amendment*, ANDY ON THE ROAD (Dec. 11, 2010, 5:31 p.m.) <http://bit.ly/gzVBfc>.

is guilty of an offence if without lawful authority he discloses any information, document or other article relating to security or intelligence which is or has been in his possession by virtue of his position as a member of any of those services or in the course of his work while the notification is or was in force.

* * *

A person who is or has been a Crown servant or government contractor is guilty of an offence if without lawful authority he makes a damaging disclosure of any information, document or other article relating to security or intelligence which is or has been in his possession by virtue of his position as such but otherwise than as mentioned in subsection (1) above.

* * *

[A] person into whose possession the information, document or article has come is guilty of an offence if he discloses it without lawful authority knowing, or having reasonable cause to believe, that it is protected against disclosure by the foregoing provisions of this Act and that it has come into his possession [as a result of disclosure by a Crown servant or government contractor] . . . without lawful authority.”¹³⁴

Assange has said of the OSA: “The dead hand of feudalism still rests on every British shoulder; we plan to remove it.”¹³⁵

While the OSA has been supplanted or amended a number of times over the years, the most recent major revision occurred during its Centenary, in 1989.¹³⁶ These enactments provided greater specificity regarding when disclosure of information is prohibited and limited penalties for unlawful disclosure to those situations in which the national interest has actually been damaged. The 1989 provisions also clarified of the scope of disclosures covered by the OSA to include information deemed vital to national security, intelligence, defense and international relations interests.

In its current form, the OSA identifies six categories of official information protected from disclosure: security and intelligence; defense; international relations; confidential

134 Official Secrets Act, 1989 c.6 § 5 (U.K.), <http://www.legislation.gov.uk/ukpga/1989/6/section/5>.

135 *Profile: Julian Assange, the man behind WikiLeaks*, THE SUNDAY TIMES (Apr. 11, 2010), <http://bit.ly/cMpH9P>.

136 Portions of the 1911 Act remain in effect after adoption of a separate Act in 1989.

information obtained from a state other than the United Kingdom or an international organization; crime; and special investigation powers. The act by its terms also applies to every citizen, including journalists, not just civil servants and government contractors.¹³⁷ While under the Espionage Act the government carries the burden of proving that a document was in fact closely held and properly a secret, the OSA requires that a defendant carry the burden of proving that a document should not be a secret.¹³⁸

Despite its apparent application to journalists, the OSA historically has, like the Espionage Act in the U.S., been applied mainly to government employees.¹³⁹ For instance, in 1983, Sarah Tisdall, a civil servant employed in the office of the Foreign Secretary, gave to *The Guardian* a memorandum reporting the date on which American cruise missiles would reach the Royal Air Force Base at Greenham Common. Although recognizing that the actual memorandum carried very little value and did not represent an attempt to undermine national security, three of five members of the House of Lords hearing the matter concluded that the evidence was sufficient for the government to continue its case. In 1984, Clive Ponting, an employee of the Ministry of Defense, leaked a document relating to the Falklands War that contradicted the government's explanation of how a British naval vessel had sunk an Argentinean cruiser, killing 360 people. The government initially prosecuted Ponting under the 1911 version of the OSA, but halfway through the trial, after acknowledging that the document did not compromise national security, retreated to a claim of breach of confidentiality. Jurors later acquitted Ponting.¹⁴⁰ More recently, in 2007, British citizen Derek Pasquill faced charges under the OSA that he made damaging disclosures after passing confidential documents to *New Statesman* magazine and *The Observer*. Pasquill was alleged to have breached the Official Secrets Act by leaking letters and memoranda about the government's attitude toward secret CIA rendition flights and contacts with Muslim groups. In 2008, however, the government withdrew its claims against Pasquill because of difficulties it faced with respect to documents it would be required to disclose as part of the legal proceedings.¹⁴¹

Unlike the Espionage Act, the OSA does not require the government to prove that a civilian recipient willfully violated the law or had an awareness of possible harm to the nation (or of benefit to its enemies), merely that the person disseminating the document knew or had reasonable cause to believe that it was an improperly leaked secret. By the same token, however, the OSA in certain circumstances requires the government to prove that the disclosure actually harmed the national security. If the U.S. diplomatic cables or war-related documents published

137 See Official Secrets Act, 1989 c.6 § 5.

138 Joseph E. Olson & David B. Kopel, *All the Way Down the Slippery Slope: Gun Prohibition in England and Some Lessons for Civil Liberties in America* 22 *HAMLIN L. REV.* 399, 440 (1999).

139 See, e.g., *Civil Servant cleared as secrets case dropped*, *THE SUNDAY TIMES* (Jan. 9, 2008), <http://bit.ly/pE75A4>.

140 Laura K. Donohue, *Terrorist Speech and the Future of Free Expression*, 27 *CARDOZO L. REV.* 233, 305-311 (2005).

141 Chris Tryhorn, 'Victory for press freedom' over leaks, *THE GUARDIAN* (Jan. 9, 2008, 12:58 GMT), <http://bit.ly/ptEGTS>.

by WikiLeaks had instead belonged to Her Majesty's government, it is not difficult to imagine the government satisfying its burden of proof on both of these points.

Moreover, currently, there is no established doctrine of British or European law equivalent to the U.S. First Amendment that might require a British court to apply limiting gloss to the statutory language. The closest analogous provision is Article 10 of the European Convention of Human Rights, which was incorporated into U.K. law by the Human Rights Act of 1998. Article 10 provides, in pertinent part:

Everyone has the right to freedom of expression. This shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiersThe exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or the rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.¹⁴²

Despite its declaration of “freedom of expression,” however, Article 10 at least arguably would have only limited application if disclosure of state secrets were at issue. As expressly stated, this “freedom” is restricted by “such formalities, conditions, restrictions or penalties as prescribed by law and . . . in the interests of national security,” a provision the British government could be expected to invoke were its own secrets at issue.

IV. WIKILEAKS AND THE FOURTH ESTATE

While American and international news organizations continue to debate the potential impact on them were Assange to be indicted under the Espionage Act, there are more immediate, practical reverberations from WikiLeaks being absorbed by the Fourth Estate. WikiLeaks' own model has changed since 2007, moving from the simple, unfiltered posting of documents on a website that encouraged user participation and editing, to a more traditional model of publishing, and one that includes development of partnerships with established news organizations. WikiLeaks' latest release, the files related to Guantanamo Bay detainees, involved partnerships with the *Washington Post*, McClatchy, Spain's *El Pais*, France's *Le Monde*, Germany's *Der Spiegel* and the U.K.'s *Daily Telegraph*. (Noticeably absent from that list were WikiLeaks' earlier partners, *The New York Times* and *The Guardian*, who were left to obtain the documents independently, and did so.)

142 Council of Europe, Convention for the Protection of Human Rights and Fundamental Freedoms, <http://conventions.coe.int/treaty/en/Treaties/Html/005.htm>.

That some news organizations have recently relied on their own sources for documents also provided to WikiLeaks begs the question of whether mainstream media organizations will be able to or want to emulate WikiLeaks' technology. Dow Jones' *Wall Street Journal* is the first major newspaper to implement a model for acquisition of information similar to WikiLeaks, having made public earlier this year a secure, electronic document drop box, dubbed "SafeHouse."¹⁴³ SafeHouse, the newspaper explains, allows anyone to upload documents directly to a secure server accessible only to high-ranking Journal editors.¹⁴⁴ The *Journal* explains the value of such a system on the SafeHouse website:

Documents and databases. They're key to modern journalism. But they're almost always hidden behind locked doors, especially when they detail wrong doing such as fraud, abuse, pollution, insider trading, and other harms. That's why we need your help. If you have newsworthy contracts, correspondence, emails, financial records or databases from companies, government agencies or non profits, you can send them to us using the SafeHouse service.¹⁴⁵

Very similar sentiments are expressed by WikiLeaks on the portion of its site describing its secure submission system. One notable difference between SafeHouse and WikiLeaks, however, can be found in SafeHouse's Terms of Use, which warn that "we cannot ensure complete anonymity."¹⁴⁶ Indeed, sources who submit documents must "agree not to use SafeHouse for any unlawful purpose," and represent that they "have all the necessary legal rights to upload or submit such Content and it will not violate any law or the rights of any person."¹⁴⁷ Furthermore, while leaving the door open to a reciprocal "confidential relationship," the *Journal* through SafeHouse also reserves the right to "disclose any information about [the source] to law enforcement authorities or to another third party without notice, in order to comply with any applicable laws and/or requests for legal process."¹⁴⁸ Some commentators have observed that these terms of service essentially "rule[] out all classified government documents (and even unclassified documents that a would-be-source is not authorized to disclose)" as well as leaks of documents belonging to private companies, as such materials likely would be copyrighted or possibly constitute trade secrets.¹⁴⁹

143 Peter Scheer, *Can Mainstream Media Match WikiLeaks? Not Likely*, HUFFINGTON POST (May 16, 2011, 6:49 pm ET) <http://huff.to/ihZqr4>.

144 *Id.*

145 *SafeHouse: Securely share information with The Wall Street Journal*, THE WALL STREET JOURNAL, <https://www.wsjsafehouse.com/>.

146 *Terms of Use for SafeHouse*, THE WALL STREET JOURNAL, <https://www.wsjsafehouse.com/terms.html>.

147 *Id.*

148 *Id.*

149 Scheer, *supra* note 144.

Nevertheless, if SafeHouse proves successful, other media organizations may follow suit, making WikiLeaks a competitor rather than a necessary source. Indeed, Al-Jazeera has launched an in-house version of WikiLeaks, called the “Transparency Unit,” which encrypts file submissions from anonymous leakers. *The New York Times*’ Bill Keller recently announced his vision of an online “EZ Pass lane for leakers,” while the *Washington Post* is also reported to be considering development of a rival system, and other regional WikiLeaks imitators have recently emerged, including Balkanleaks, Indoleaks and Brusselsleaks.¹⁵⁰

As unauthorized disclosures become increasingly decentralized on the Internet, Assange may to some extent become old hat. Yet, it remains to be seen whether new outlets will be willing to take the risks and publish the same documents that have found public release on www.wikileaks.org, and whether sources of such documents will be as comfortable with mainstream news organizations or new enterprises as they are with Assange: “WikiLeaks is a rogue news outlet that is both stateless and virtual. Unfortunately for mainstream media, those characteristics give it a leg up in protecting confidential documents and sources.”¹⁵¹ And it remains to be seen both whether U.S. prosecutors will seek or obtain an indictment against Assange or WikiLeaks and, if so, whether such charges can be circumscribed in a way that leaves mainstream news organizations positioned differently under the Espionage Act.

150 Dana Rosenblat, *Wiping away whistle-blowers’ online fingerprints*, CNN TECH (June 11, 2011), <http://bit.ly/njA9ed>.

151 Scheer, *supra* note 144.