UNC SCHOOL OF LAW

NORTH CAROLINA JOURNAL OF LAW & TECHNOLOGY

Volume 12
Issue 3 *Online Issue*

Article 8

10-1-2010

The Espionage Act and Today's High-Tech Terrorist

Jamie L. Hester

NORTH CAROLINA JOURNAL OF LAW & TECHNOLOGY
12 N.C. J.L. & TECH. ON. 177 (2011)

THE ESPIONAGE ACT AND TODAY'S "HIGH-TECH TERRORIST"

Jamie L. Hester*

Throughout the twentieth century courts interpreted the Espionage Act of 1917 to criminalize leaking classified information, but consciously refused to extend the Act to prohibit press institutions from subsequently publishing leaked information. While the United States government has a significant interest in preventing dissemination of sensitive information, the courts allow news organizations to claim First Amendment protection to foster government transparency and public disclosure. The proliferation of digital media, highlighted by the recent exposure of WikiLeaks founder Julian Assange, presents an additional challenge to refine characteristics of press institutions to determine if online news organizations will qualify for the same First Amendment protections. Beyond the potential prosecution of Assange in American courts, both Houses of Congress are considering the SHIELD Act, a bill that would broaden the statutory language of the Espionage Act and facilitate targeting of publishers of classified information.

I. INTRODUCTION

The reach of the United States' criminal authority in the international sphere has roots in the Espionage Act of 1917[1] ("Act"). Since its inception the U.S. government has used the Act to pursue and prosecute American citizens, and later foreign nationals, acting against the interests of the United States' national security.[2] Provisions of the Act were first used to criminalize sharing sensitive information with foreign governments, but later the U.S. government used the Act to prosecute leaks to the press

* J.D. Candidate, University of North Carolina School of Law, 2012.

[1] 18 U.S.C. §§ 792–798 (2006).

[2] *See, e.g.*, New York Times Co. v. United States, 403 U.S. 713 (1971); United States v. Zehe, 601 F. Supp. 196 (D. Mass. 1985).

and attempted to target the media publishing such leaked information.[3] The recent arrest of WikiLeaks[4] founder Julian Assange in Great Britain, after he led efforts to release secret cables and documents from the United States military and foreign service, has raised the possibility that the United States might seek his extradition to prosecute him for espionage.[5] Under the Espionage Act, acquiring and transmitting classified United States intelligence are crimes, though the Supreme Court has recognized safe havens for the press and publishers to protect the rights enshrined in the First Amendment.[6] It is not clear if the current interpretation of the Act would give exception to Assange's publication if the U.S. government prosecuted him under the Act since his role as WikiLeaks founder and leader could be viewed as outside the scope of a traditional journalist. With Assange's potentially illegal acts of espionage playing out on a digital stage, technology has serious implications for defining the role of a journalist.

Anticipating the lack of clarity, U.S. legislators recently introduced legislation in both the House of Representatives and the Senate to broaden the definition and scope of espionage, encompassing not only the leaking of classified information but also the publication of such data.[7] Passage of the Securing Human

---

[3] *See* Jereen Trudell, *The Constitutionality of Section 793 of the Espionage Act and Its Application to Press Leaks*, 33 WAYNE L. REV. 205, 210–14 (1986) (citing United States v. Morison, 604 F. Supp. 655 (D. Md. 1985) (describing the history of application of the Act to the press, focusing on *United States v. Morison*, in which the District Court of Maryland concluded that there is no immunity from the Espionage Act for those who leak information to journalists)).

[4] WIKILEAKS, http://213.251.145.96/ (last visited Feb. 13, 2011).

[5] Peter Grier, *Julian Assange: Extradition to Sweden just a stop en route to US?*, THE CHRISTIAN SCI. MONITOR (Feb. 24, 2011), http://www.csmonitor.com/USA/2011/0224/Julian-Assange-Extradition-to-Sweden-just-a-stop-en-route-to-US.

[6] *See* Trudell, *supra* note 3.

[7] *See* S. 4004, 111th Cong. (2010) (amending § 798 of title 18 of the United States Code, a provision of the Espionage Act); H.R. 6506, 111th Cong. (2010) (same); *see also* S. 315, 112th Cong. (2011) (reintroducing the SHIELD Act amendment in the current Congress); H.R. 703, 112th Cong. (2011) (same).

Intelligence and Enforcing Lawful Dissemination ("SHIELD") Act would make successful conviction more likely. However, it would also throw the current balance between illegal espionage and investigative journalism, a line both the Supreme Court and lower courts have drawn between national security interests and freedom of the press, into dangerous disarray.

In Part II, this Recent Development will examine the Espionage Act's text and its treatment in American courts during the twentieth century, including application not only to American citizens located domestically and abroad, but also to foreign nationals allegedly acting against U.S. national security interests. This paper will grant particular attention to espionage cases in which freedom of the press colored the courts' opinions. In Part III, this Recent Development will examine the controversy surrounding WikiLeaks and its founder Julian Assange as an illustration of the tangled web technology has woven for applying the ambiguous provisions of the Act to online media organizations. However, as Part III will highlight, the recently introduced SHIELD Act purports to clarify some of those existing ambiguities and broaden the types of espionage criminalized by the Espionage Act, a move that indicates the direction of not only the judiciary but also the U.S. Congress. This Recent Development will conclude by recognizing the uncertain distinction of Assange as a journalist and propose that with the current interpretations of protections for media organizations he could evade conviction.

II. THE ESPIONAGE ACT OF 1917

A. *Statutory Language*

The Espionage Act of 1917[8] was passed during wartime to target individuals working against the interests of American

[8] The Espionage Act, 18 U.S.C. §§ 792–798 (2006). For a detailed recitation of the legislative history and statutory language of the Espionage Act, now codified in §§ 792–798, *see generally* Harold Edgar and Benno C. Schmidt, Jr., *The Espionage Statutes and Publication of Defense Information*, 73 COLUM. L. REV. 929 (1973). The article was published soon after the Supreme Court case of *New York Times v. United States* in the early 1970's, but its thorough explication of the legislative intent is still applicable.

national security.[9] For purposes of this Recent Development, the "Act" refers to §§ 792–798 of Title 18 of the United States Code, though certain provisions of § 793[10] and § 798[11] are the most applicable to the taking, transmission, and dissemination of documents that threaten U.S. national security. Section 793(b) specifically prohibits copying, taking, or obtaining documents "connected with the national defense," or attempting to do any of the above, "for the purpose of obtaining information respecting the national defense with intent or reason to believe that the information is to be used to the injury of the United States or to the advantage of any foreign nation."[12] In § 793(c), reception of such information, with the same intent as in subsection (b), is a criminal act.[13] Section 793(e) criminalizes willful communication and transmission of information by any person having "unauthorized possession of access to or control over" documents and information "relating to the national defense."[14] These three subsections are particularly applicable to actions of leakers of information and also could include the actions of publishers.

In contrast, § 798(a), added to the Act in 1951, states:

> Whoever knowingly and willfully communicates furnishes transmits or otherwise makes available to an unauthorized person or publishes or uses in any manner prejudicial to the safety or interest of the United States or for the benefit of any foreign government to the detriment of

---

[9] *See* Geoffrey R. Stone, *Free Speech and National Security*, 84 IND. L.J. 939, 944–46 (2009) (providing an analysis of the background of the Espionage Act and free speech). Professor Stone points out that the Espionage Act was initially used with fervor when applied to war dissenters, through the beginning of World War II. *Id.*

[10] 18 U.S.C. § 793 (criminalizing the gathering, transmitting, or losing of defense information with the purpose of injuring the United States or providing advantage to a foreign government, including conspiracy or attempt to do the same).

[11] *Id.* § 798 (criminalizing the disclosure of classified information if detrimental to the security of the United States, specifically including the publishing of such information).

[12] *Id.* § 793.

[13] *Id.*

[14] *Id.*

> the United States [specific types of classified information will be criminally liable].[15]

Such classified information, as the law currently reads, relates specifically to use of codes, ciphers, communication intelligence activities, or obtained through communication intelligence activities of foreign governments.[16] While § 793 has a broad conception of classified information (such that it is related or connected to national defense), the more recently formulated § 798 has a lower threshold for intent (such that it is detrimental to the interests of the United States) and specifically mentions publishing.

Under the Espionage Act, the United States criminalizes acts of espionage by American citizens inside and outside U.S. borders and acts of espionage by foreign nationals that occur within the United States. Recently, courts have interpreted the Act even more liberally, allowing the prosecution of foreign nationals outside the jurisdiction of the United States proper.[17] Thus, the United States has not limited its jurisdiction by geographic location or nationality of the suspected criminal, but instead has focused on the nature of the act itself since the act is the source of the harm to national security interests.

A. *Application and Interpretation*

1. *Criminalizing Publication*

The U.S. government's first significant use of the Act occurred in 1919 when used against American citizens who passed out leaflets that derided conscription and compared it to slavery.[18] Finding that there was a sufficiently clear and present danger in publishing the information to uphold the defendants' convictions, the Supreme Court said that the Espionage Act did allow prosecution of such behavior, despite First Amendment concerns and the abrogation of free speech.[19]

---

[15] *Id.* § 798.
[16] *Id.*
[17] *See* United States v. Zehe, 601 F. Supp. 196, 197 (D. Mass. 1985).
[18] Schenck v. United States, 249 U.S. 47, 49–50 (1919).
[19] *Id.* at 52.

The Espionage Act was used perhaps most famously in the 1970's to stop the publication of the Pentagon Papers in *The New York Times* and *The Washington Post*.[20] The so-called "Pentagon Papers" "consisted of forty-seven volumes totalling [sic] 7,000 pages containing 2.5 million words,"[21] published by *The New York Times* in a series of excerpts in 1971.[22] These papers documented the United States' extensive involvement in Southeast Asia in the 1960's, information some government officials viewed as harmful to U.S. security interests, sufficient to require the U.S. District Court for the Southern District of New York to order an injunction against publication.[23] The Supreme Court determined that the U.S. government had not met its burden to continue the injunction against *The New York Times* and *The Washington Post*, but made no definite ruling on the application of the Espionage Act to the papers' publications after the fact.[24] However, Justice Douglas wrote a concurring opinion, joined by Justice Black, in which he explicitly recognized that if the government had invoked the Espionage Act statutes in their arguments to uphold the injunction, the specific inclusion of "publishes" versus "communicates" in various subsections of § 794, § 797, and § 798 showed Congressional intent to "distinguish between publishing and communication in the various sections of the Espionage Act."[25] At trial, the U.S. government had indeed used § 793(e) to support its injunction against *The New York Times*, but the District Court of New York firmly rejected the government's contention that prohibitions against communication of sensitive information

---

[20] *See* Melville B. Nimmer, *National Security Secrets v. Free Speech: The Issues Left Undecided in the Ellsberg Case*, 26 STAN. L. REV. 311, 312–13 (1974) (describing the facts of *New York Times Co. v. United States* as well as the background of the U.S. case against the individuals accused of procuring the classified documents, Daniel Ellsberg and Anthony Russo, in *United States v. Russo*).

[21] John Cary Sims, *Triangulating the Boundaries of Pentagon Papers*, 2 WM. & MARY BILL RTS. J. 341, 357 (1993).

[22] *Id.* at 355–57 (1993). The article notes that *The New York Times* was enjoined from publishing the documents for a brief period in June. *Id.* at 355.

[23] *Id.*

[24] New York Times Co. v. United States, 403 U.S. 713, 714–15 (1971).

[25] *Id.* at 720–22 (Douglas, J., concurring).

covered publication by a newspaper, once information was already leaked.[26] In reference to § 793(e), the District Court held that "what is prohibited is the secret or clandestine communication to a person not entitled to receive it" while "in other sections of Chapter 37 [including §§ 794 and 798] there is specific reference to publication."[27] The U.S. government opted not to use the Espionage Act at the appellate level, so the Supreme Court did not rule on the question of application of the Espionage Act to newspaper publishers.[28]

The next significant case in which sharing classified military documents with members of the press presented a central question for the courts was *United States v. Morison*.[29] In *Morison*, an analyst at the Naval Intelligence Support Center took classified pictures and transmitted them to an editor of a British magazine, for whom Morison also worked.[30] The Fourth Circuit ruled that Morison had violated § 793(d) of the Espionage Act, but only because he was a government official who shared sensitive military photographs with the press.[31] The court avoided a ruling on exactly how the Espionage Act could be used to prosecute journalists, and it did not consider Morison's employment as a journalist of the magazine as a factor relevant to his liability.[32]

In a concurring opinion, Judge Wilkinson recognized that the majority opinion failed to fully appreciate the balancing act between freedom of the press and national security interests.[33] He emphasized that freedom of the press is vital to a functioning democratic government and drew the court's attention to *The Washington Post*'s amicus curiae brief as emblematic of the

---

[26] United States v. New York Times Co., 328 F. Supp. 324, 328 (S.D.N.Y. 1971).
[27] *Id.*
[28] *New York Times*, 403 U.S. at 714.
[29] 844 F.2d 1057 (4th Cir. 1988).
[30] *Id.* at 1060–61.
[31] *Id.* at 1070.
[32] Laura Barandes, *A Helping Hand: Addressing New Implications of the Espionage Act on Freedom of the Press*, 29 CARDOZO L. REV. 371, 394 (2007).
[33] *Morison*, 844 F.2d at 1084 (Wilkinson, J., concurring).

benefits of a free press.[34] A decision against Morison, the *Post* cautioned and Wilkinson reiterated, would "affect and perhaps dramatically alter the way in which government officials deal with the press the way in which the press gathers and reports the news and the way in which the public learns about its government"[35] Wilkinson lamented that even in the face of national security concerns, "[c]riminal restraints on the disclosure of information threaten the ability of the press to scrutinize and report on government activity. . . . We have placed our faith in knowledge, not in ignorance, and for most, this means reliance on the press."[36] Judge Wilkinson noted that "investigative reporting is a critical component of the First Amendment's goal of accountability in government. To stifle it might leave the public interest prey to the manifold abuses of unexamined power."[37] Although the court did not afford Morison any First Amendment protections against prosecution under the Espionage Act, the concurring opinion recognized the weighty significance of freedom of the press even in the face of national security threats.

As illustrated above, United States courts have recognized a distinction between the leaking of sensitive military information to journalists and the publication of the same by press institutions. As of this writing, the U.S. government has yet to successfully convict a journalist or media organization for publishing classified information.[38] Members of the Executive Branch, however, have

---

[34] *Id.* at 1080–81.

[35] *Id.* (quoting Brief for Washington Post et al. as Amici Curiae, United States v. Morison, 844 F.2d 1057 (1988)). Judge Wilkinson also quoted James Madison to emphasize society's interest in promoting civic discourse and access to government information: "'A popular Government, without popular information, or a means of acquiring it, is but a Prologue to a Farce or a Tragedy; or, perhaps both.'" *Id.* at 1081 (quoting 9 JAMES MADISON, THE WRITINGS OF JAMES MADISON COMPRISING HIS PUBLIC PAPERS AND HIS PRIVATE CORRESPONDENCE, INCLUDING NUMEROUS LETTERS AND DOCUMENTS NOW FOR THE FIRST TIME PRINTED 103 (Gaillard Hunt ed., 1910)).

[36] *Id.*

[37] *Id.*

[38] *Espionage Act and the Legal and Constitutional Issues Raised by WikiLeaks: Hearing on H.R. 6506 Before the H. Comm. on the Judiciary*, 111th

suggested that such convictions are not out of the question.[39] In 2006, when discussing an ongoing espionage case against two lobbyists working for the American Israel Public Affairs Committee,[40] then Attorney General Alberto Gonzales hinted that, like the two lobbyists, *The New York Times* could be criminally liable for publication of classified documents.[41] Fellow Justice Department officials later confirmed that the Attorney General's comments referred to applying the text of the Espionage Act specifically to journalists.[42] Although the Supreme Court has yet to rule on the precise scope of protections afforded media organizations, courts have respected a significant degree of protection for journalists that publish already leaked information as compared to those individuals who illegally acquire and leak classified documents.[43]

2. *Espionage Act as Applied to Foreign Nationals*

In 1985, the United States District Court for the District of Massachusetts ruled that the Espionage Act did more than criminalize the leaking of classified information by *American* citizens.[44] *United States v. Zehe*[45] held that the Act provided the United States authority to criminalize and prosecute acts of foreign nationals in foreign jurisdictions as well.[46] The court did not interpret the scope of the Espionage Act as only targeting Americans, but instead viewed it as a broad protective measure

---

Cong. 39 (2010) [hereinafter *Hearing*] (statement of Kenneth L. Wainstein, Partner, O'Melveny & Myers, LLP).

[39] Derigan A. Silver, *National Security and the Press: The Government's Ability to Prosecute Journalists for the Possession or Publication of National Security Information*, 13 COMM. L. & POL'Y 447, 448–449 (2008).

[40] *See* Jonathon H. Adler & Michael Berry, *A Troubling Prosecution,* NAT'L REV. ONLINE (Aug. 21, 2006), http://www.nationalreview.com/articles/218521/troubling-prosecution/jonathan-h-adler (describing the First Amendment and freedom of the press concerns in light of the case *United States v. Rosen*).

[41] Silver, *supra* note 39.

[42] *Id.* at 449.

[43] *Hearing*, *supra* note 38, at 17 (statement of Geoffrey R. Stone, Professor and former Dean, University of Chicago Law School).

[44] United States v. Zehe, 601 F. Supp. 196 (D. Mass. 1985).

[45] *Id.*

[46] *Id.* at 198.

that criminalized certain acts contrary to the interests of the United States.[47] The court held that the invocation of the Espionage Act depends on the nature of the act rather than the person who committed the act, since the action threatens the national security of the United States.[48] The *Zehe* court relied on precedent when it observed that previous "courts expressly relied upon the nature of the offenses, and not just upon the citizenship of the defendants."[49] The defendant, who was a German, argued that the Act was not meant to apply to "noncitizens acting entirely outside of the United States."[50] Furthermore, "in order to apply a criminal statute to acts committed by noncitizens beyond this country's territorial boundaries, there must be a strong and clear showing of congressional intent."[51] The court rejected the defendant's argument with a textualist construction; the Act said nothing about applying only to American citizens or, more importantly here, to acts that occurred within the country's territories.[52]

Given courts' decisions to apply the Espionage Act based on the offense regardless of the status of the person who committed it, individuals suspected of espionage cannot find refuge in foreign jurisdictions.[53] Therefore, any attempts to prosecute individuals

---

[47] *Id.* at 197.

[48] *Id.*

[49] The previous decisions referred to in the *Zehe* case are United States v. Bowman, 260 U.S. 94 (U.S. 1922); United States v. Cotten, 471 F.2d 744 (9th Cir. 1973); and United States v. Birch, 470 F.2d 808 (4th Cir. 1972). According to the *Zehe* court, all three cases held that criminal offenses against the U.S. government depended on the offense itself, not the source of the offense, such as a noncitizen. *Zehe*, 601 F. Supp. at 197.

[50] *Id.* at 198.

[51] *Id.*

[52] *Id.* The Espionage Act states that "whoever knowingly and willfully communicates . . . to an unauthorized person" the classified information should be fined or imprisoned, or both. It does not specify the citizenship of the person committing espionage. 18 U.S.C. § 798(a) (2006).

[53] The Espionage Act is not the only statutory authority that extends criminal jurisdiction beyond the territories of the United States. For example, the Military Extraterritorial Jurisdiction Act expands United States criminal jurisdiction over foreign nationals acting under the purview of the United States, such as military contractors. Extension of jurisdiction over foreign nationals acting on foreign soil is not a particularly unusual possibility. See K. Elizabeth

who publish sensitive documents would not be hindered by the fact that the alleged crimes occurred on the Internet or in a foreign jurisdiction.

III. JULIAN ASSANGE AND THE WIKILEAKS CONTROVERSY

A. *The Intelligence Leak*

In the summer of 2010, Julian Assange and fellow Internet activists met in Iceland to decrypt sensitive military video footage, which revealed a 2007 incident in which an American Apache military helicopter[54] fired on civilians in Iraq.[55] Assange's project, WikiLeaks, had been operating for years, but this was the first big release of sensitive data, and it jettisoned Assange and WikiLeaks into the public eye.[56] Later, it became apparent that Assange and his team desired more than posting only one damaging video. Shortly after releasing the decrypted video of the military attack, the WikiLeaks group published tens of thousands of sensitive documents and "classified cables"[57] on their Web site, which

---

Waits, *Avoiding the "Legal Bermuda Triangle": The Military Extraterritorial Jurisdiction Act's Unprecedented Expansion of U.S. Criminal Jurisdiction Over Foreign Nationals*, 23 ARIZ. J. INT'L & COMP. LAW 493 (2006), for a detailed analysis of the United States' criminal jurisdiction over individuals acting in connection with U.S. military forces.

[54] *Boeing: AH-64 Apache*, BOEING (last visited Jan. 28, 2011), http://www.boeing.com/rotorcraft/military/ah64d/index.htm (describing the specifications of the AH-64A Apache helicopter used by military customers).

[55] Raffi Khatchadourian, *No Secrets*, THE NEW YORKER, (June 7, 2010), http://www.newyorker.com/reporting/2010/06/07/100607fa_fact_khatchadourian.

[56] Noam Cohen and Brian Stelter, *Iraq Video Brings Notice to a Web Site*, N.Y. TIMES (Apr. 6, 2010), http://www.nytimes.com/2010/04/07/world/07wikileaks.html; Steve Kingstone, *WikiLeaks posts video of 'US military killings' in Iraq*, BBC NEWS (Apr. 6, 2010), http://news.bbc.co.uk/2/hi/americas/8606402.stm; Declan McCullagh, *Wikileaks releases video of Iraq journalist shooting*, CNET.COM (Apr. 5, 2010), http://news.cnet.com/8301-13578_3-20001802-38.html?tag=mncol; *Iraqi journalists want probe of taped US shooting*, FOX NEWS (Apr. 6, 2010), http://www.foxnews.com/world/2010/04/06/iraqi-journalists-want-probe-taped-shooting/.

[57] The "classified cables" refer to "the kinds of cables that [diplomatic] posts send to Washington" that "involve discussions that [diplomats] had with

incriminated not only the United States, but a host of other countries in behind-closed-door deals and duplicitous maneuverings.[58]

The United States government, alarmed at the massive release of secret diplomatic cables and military information, initially pursued the leak among military personnel.[59] Private Bradley Manning, a serviceman in the U.S. Army, was arrested and charged under military law for downloading the intelligence data onto a digital memory stick, transferring those data to his own computer, and sending the information to an unauthorized source.[60] The purely technological transfer presented a new, tougher problem for the United States government than previous intelligence leaks like the belabored copying of the Pentagon Papers in the 1970's.[61]

The ease of transfer and subsequent publication of tens of thousands of documents en masse over the Internet has raised

---

government officials, with private citizens." The U.S. State Department feared that release of the cables would "create tension in our relationships between our diplomats and our friends around the world." Daily Press Briefing, Philip J. Crowley, Assistant Secretary, U.S. Department of State, http://www.state.gov/r/pa/prs/dpb/2010/11/151962.htm (Nov. 24, 2010).

[58] Khatchadourian, *supra* note 55.

[59] U.S. investigations focused internally on the military to out the leakers when the video of the Apache helicopter attack on civilian journalists was first released. Thousands of documents related to the U.S. involvement in Afghanistan were released on WikiLeaks, and the U.S. government then sought to expand its criminal investigations into the WikiLeaks organization. *See* Phil Stewart, *WikiLeaks has more U.S. war files, Pentagon says*, REUTERS (Oct. 26, 2010), http://www.reuters.com/article/2010/10/26/us-wikileaks-iraq-pentagon-idUSTRE69P4S220101026.

[60] Chris McGreal, *US private Bradley Manning charged with leaking Iraq killings video*, THE GUARDIAN (Jul. 6, 2010), http://www.guardian.co.uk/world/2010/jul/06/bradley-manning-charged-iraq-killings-video. For more information about Manning's own thoughts on the ease of the digital transfer, see David Leigh, *How 250,000 US embassy cables were leaked*, THE GUARDIAN (Nov. 28, 2010), http://www.guardian.co.uk/world/2010/nov/28/how-us-embassy-cables-leaked.

[61] *See* Nimmer, *supra* note 20; William H. Freivogel, *Feds take unusual step of subpoenaing Sterling's lawyer*, ST. LOUIS BEACON (Jan. 21, 2011), http://www.stlbeacon.org/issues-politics/nation/107662-sterling-lawyers-subpoena.

concerns about the blurring line between press and leaker.[62] Also, in addition to the ease of transfer, it is possible that universal access to such information contributes to the security threat when it is posted online, since the recipient could be any foreign government or terrorist organization. When news of the intelligence leak reverberated in public, members of Congress, as well as the Obama Administration, denounced the unauthorized publications as the work of a terrorist.[63] Senator Dianne Feinstein called for prosecution of Assange specifically under the Espionage Act.[64]

B. *The Espionage Act and Online Media Organizations*

Condemnation of Julian Assange and his WikiLeaks cohorts progressed to prosecution efforts by the U.S. government, likely under the Espionage Act. The actions of Assange and WikiLeaks have raised questions about the application of the Act, a law that now dates back nearly 100 years and contains ambiguous references to "information respecting the national defense"[65] and

---

[62] In his report filed when testifying before the House Judiciary Committee on the proposed SHIELD Act, attorney Abbe Lowell said that differing interpretations of "communication," "publication," and "use," as set forth in § 798, fail to realize that "digital technology and the Internet have significantly blurred, if not entirely erased, the lines" between the three terms. *Espionage Act and the Legal and Constitutional Issues Raised by WikiLeaks: Hearing on H.R. 6506 Before the H. Comm. on the Judiciary*, 111th Cong. 29 (2010) (statement of Abbe D. Lowell, Partner, McDermott Will & Emery, LLP).

[63] John Bingham, *WikiLeaks: Julian Assange facing US prosecution bid, says Joe Biden*, THE TELEGRAPH (Dec. 19, 2010), http://www.telegraph.co.uk/news/worldnews/wikileaks/8212812/WikiLeaks-Julian-Assange-facing-US-prosecution-bid-says-Joe-Biden.html.

[64] Dianne Feinstein, *Prosecute Assange under the Espionage Act*, WALL ST. J. (Dec. 7, 2010), http://online.wsj.com/article/SB10001424052748703989004575653280626335258.html (stating that Assange "is no journalist: He is an agitator intent on damaging our government. . . ." and should not be given any protection under the First Amendment).

[65] 18 U.S.C. § 793(a) (2006) (offering no definition of "respecting national defense").

"classified information."[66] Vice President Joseph Biden claimed that the U.S. is pursuing prosecution of Assange for his involvement in the WikiLeaks acquisition and release of classified information, but the potential charges are as of yet unclear.[67] Biden called Assange a "high-tech terrorist,"[68] drawing attention to the Administration's interpretation of WikiLeaks' actions as a form of technological warfare, not a form of investigative journalism.

The online publication of government secrets raises a slew of new legal questions for the U.S. government to answer in its quest to pin Assange with charges of espionage in connection to the classified information stolen by Manning and the publication of such documents on the WikiLeaks Web site.[69] The United States has not used the Espionage Act in the past to criminalize publication of classified information; instead it has pursued those who leaked the secret documents or exchanged them with the press.[70] Thus, WikiLeaks' publication of thousands of such documents in the name of government transparency and public disclosure requires a look at the courts' willingness to afford WikiLeaks and similar online media organizations the same consideration they have for traditional news institutions like *The New York Times*, *The Washington Post*, and *The Chicago Tribune*.

The status of WikiLeaks as a clearinghouse of secured documents and a publisher of such information makes it a vulnerable target for the Espionage Act. Julian Assange's role in the leaking and publication is in question, because although he acted primarily as a publisher, he also may have acquired,

---

[66] 18 U.S.C. § 798(b) (defining "classified information" as "information which . . . is, for reasons of national security, specifically designated by a United States Government Agency for limited or restricted dissemination or distribution).

[67] *See* Bingham, *supra* note 63.

[68] *Id.*

[69] Julian E. Barnes & Evan Perez, *Assange Probe Hits Snag*, WALL ST. J. (Feb. 9, 2011), http://online.wsj.com/article/SB10001424052748703313304576132543747598766.html?mod=WSJ_hp_MIDDLENexttoWhatsNewsThird.

[70] *Assange charges center on two women, sex*, MSNBC (Dec. 8, 2010), http://www.msnbc.msn.com/id/40551118/ns/us_news-wikileaks_in_security.

collected, and solicited the information, which puts him in a different position than *The New York Times* when it was offered the information in the Pentagon Papers.[71] *The New York Times* is an established newspaper, while WikiLeaks is a Web site self-proclaimed as a "non-profit media organization."[72] Scholars have suggested that even *The New York Times* could have faced prosecution under the Espionage Act for retaining, accumulating, and discussing the potentially threatening materials in the Pentagon Papers.[73]

The line drawn by the courts between the leaking of information and the publishing of information could break down when applied to the facts of a potential U.S. suit against WikiLeaks and Julian Assange. The U.S. Department of State sent Assange a letter dated November 27, 2010, warning the online activist that publishing the classified diplomatic cables would be a danger to "innocent individuals."[74] The letter also informed Assange that he violated U.S. law merely by retaining such documents, an early hint that the U.S. could build a criminal case against him given the Espionage Act's prohibitions against acquiring and retaining secret documents.[75]

The U.S. government, if it pursued criminal charges against Assange, would likely allege that he violated both § 793(b) (which makes it illegal to copy or obtain sensitive materials) and § 793(e) (which makes it illegal for those with unauthorized possession to communicate or transmit sensitive materials). The courts could rule that Assange's publication of the secret documents is protected by the First Amendment, and that publication by media organizations would not satisfy § 793(e)'s requirement that one

---

[71] William H. Freivogel, *Feds take unusual step of subpoenaing Sterling's lawyer*, ST. LOUIS BEACON (Jan. 21, 2011), http://www.stlbeacon.org/issues-politics/nation/107662-sterling-lawyers-subpoena.

[72] WIKILEAKS, http://213.251.145.96/ (last viewed Feb. 13, 2011).

[73] Harold Edgar & Benno C. Schmidt, Jr., *The Espionage Statutes and Publication of Defense Information*, 73 COLUM. L. REV. 929, 967, 1036 (1973).

[74] Michael Hirsh, *'Countless Innocent Individuals' at Risk*, NAT'L J. (Nov. 28, 2010), http://nationaljournal.com/nationalsecurity/state-dept-countless-innocent-individuals-at-risk-20101128?mrefid=site_search.

[75] *Id.*

must *willfully* communicate, deliver, or transmit documents related to national defense. However, as U.S. officials and scholars have suggested, Assange and other WikiLeaks employees could be criminally liable if they merely obtained the information from a source known to have copied the data illegally, and had the requisite intent or reason to believe the information could be used to the detriment of the United States.[76]

If the U.S. government were to file a lawsuit against Assange, the courts could rule that simply because WikiLeaks and Assange himself acquired, retained, and transmitted the information, then the organization and the individual violated the Espionage Act. Such a ruling would, of course, depend on the requisite intent to injure the United States' national security interests and proof that Assange directly enabled the dissemination. While courts have been hesitant to directly state that news organizations have immunity from the Espionage Act by merely reporting on leaks already made by third parties, precedent suggests that judges would be sympathetic to WikiLeaks. In *Morison*, Judge Wilkinson recognized the role of the press "to scrutinize and report on government activity," to foster "knowledge," and to expose government abuses of power.[77] WikiLeaks, despite being publicly condemned as a terrorist organization or labeling as a group of hacker activists, gathered the secured documents and reported on them in the interest of public disclosure. Assange and his team preemptively contacted the U.S. Department of State to collaborate on the thousands of documents they planned to reveal, and they published a selection of the materials received from P.F.C. Manning.[78] Even *The Guardian*, a London-based print and online newspaper,[79] sifted through the database of classified information and published their own selection with redactions of information they thought might harm individuals.[80] WikiLeaks also parsed

---

[76] Edgar & Schmidt, *supra* note 73, at 967 and 1036.

[77] United States v. Morison, 844 F.2d 1057, 1081 (4th Cir. 1988).

[78] *See* Leigh, *supra* note 60.

[79] *The Guardian* is the online version of *The Observer*, its sister paper. *See User FAQ*, THE GUARDIAN (last visited Feb. 24, 2011), http://www.guardian.co.uk/help/users/faq#newspaper.

[80] *Id.*

through the information like its more traditional media counterpart. These factual parallels would likely bolster WikiLeaks' argument before American courts that it was acting in the interests of public disclosure and government scrutiny, even at the risk of the U.S. government suffering embarrassment, injured diplomatic relations, and additional threats to military activities.

C. The *SHIELD Act: Congressional Reaction to WikiLeaks*

The U.S. government has yet to extradite and pursue prosecution of Julian Assange or any WikiLeaks employee as of this writing.[81] However, while the Justice Department is moving cautiously, the U.S. Congress has explored new legislation to vigorously pursue criminal leaks, making journalists and media organizations more likely targets.[82] The Securing Human Intelligence and Enforcing Lawful Dissemination ("SHIELD") Act was first introduced in the Senate on December 2, 2010 by Senator John Ensign (R-NV) with support from Senator Joseph Lieberman (I-CT).[83] An identical bill was introduced in the House of Representatives on December 8, 2010.[84] Both identical versions of the bill were reintroduced in the 112th Congress with a greater number of co-sponsors.[85] The WikiLeaks publication spurred Senator Lieberman's support for the bill, because an amendment of the Espionage Act is necessary to "give the Administration increased flexibility to go after WikiLeaks and its founder Julian

---

[81] On January 24, 2011, NBC News reported that Pentagon officials could not prove a sufficient connection between Private Bradley Manning and Julian Assange. However, the Attorney General suggested that prosecution under the Espionage Act was not out of the question if the U.S. government could make a case that the publication of the leaked documents was enough to constitute a crime. *See* Jim Miklaszewski, *NBC: U.S. can't link accused Army private to Assange*, MSNBC (Jan. 24, 2011), http://www.msnbc.msn.com/id/41241414/.

[82] Posting of Benjamin Wittes to Lawfare Blog (Dec. 6, 2010), http://www.lawfareblog.com/2010/12/espionage-act-amendments/ (Dec. 6, 2010, 11:40 AM).

[83] S. 4004, 111th Cong. (2010).

[84] H.R. 6506, 111th Cong. (2010).

[85] S. 315, 112th Cong. (2011) (reintroducing the SHIELD Act amendment in the current Congress); H.R. 703, 112th Cong. (2011) (same).

Assange."[86] The SHIELD Act builds on the existing language of the Espionage Act, broadening the range of activities punishable under the U.S. criminal code to include publishing the names of human intelligence informants and disclosure of information that poses a security threat to the United States.[87] Specifically, the law amends only § 798 (previously recognized to protect a narrow category of communications intelligence and cryptography) to criminalize publication of "classified information"[88] that benefits a "transnational threat."[89]

The bill is worded such that the U.S. government can more successfully prosecute Assange if his activities continue. Given the past treatment of sections of the Espionage Act in courts, it is likely that the U.S. government would rely on § 793 to pursue Assange or similar "high-tech terrorists" prior to passage of the SHIELD Act. If the SHIELD Act were enacted as currently introduced, the explicit criminality of publication already enshrined in § 798, as contrasted with the more nebulous provisions regarding publication in § 793, would enable the government to attack the WikiLeaks publications more easily under § 798. Testifying before the House Committee on the Judiciary in a hearing for the SHIELD Act, former Assistant Attorney General Kenneth Wainstein emphasized the serious threat posed by WikiLeaks:

> [WikiLeaks and similar online organizations are] a threat that will only get more dangerous with the advance of enabling technology and with

---

[86] *Bipartisan Legislation Goes After WikiLeaks by Amending Espionage Act*, JOE LIEBERMAN: UNITED STATES SENATOR FOR CONNECTICUT (Dec. 2, 2010), http://lieberman.senate.gov/index.cfm/news-events/news/2010/12/bipartisan-legislation-goes-after-wikileaks-by-amending-espionage-act.

[87] S. 4004, 111th Cong. (2010).

[88] *Id.* (defining "classified information" as "information which . . . is, for reasons of national security, specifically designated by a United States Government Agency for limited or restricted dissemination or distribution").

[89] *Id.* (defining "transnational threat" as "(A)ny transnational activity (including international terrorism, narcotics trafficking, the proliferation of weapons of mass destruction and the delivery systems for such weapons, and organized crime) that threatens the national security of the United States; or (B) any individual or group that engages in an activity referred to in subparagraph (A).").

> the realization after these recent leaks that it takes so little to strike such a grandiose blow against government secrecy—nothing more than a computer, access to a disaffected government employee with a clearance, and a willingness to compromise our nation's interests and security.[90]

As a nascent media organization, WikiLeaks fails to show the same self-governance as a newspaper like *The New York Times* or *The Washington Post*, or even *The Guardian*, institutions that risk public backlash and lawsuits if they publish overly sensitive national security information that is not essential to government transparency. As precedent shows, the judiciary and legislature have accepted the status quo balance between freedom of the press and national security with respect to the publication of leaked classified documents. However, the burgeoning area of online media adds another outlet for leaks in a form that might lack internal policing procedures to reduce the threat of publishing truly dangerous information. WikiLeaks, unlike its inked contemporaries, functions as a digital clearinghouse willing to post information online without the same degree of screening for dangerous information. If WikiLeaks fails to convince legislators that it is a legitimate news organization acting in the public interest to examine hidden government activities, then Congress will likely pass the SHIELD Act or similar amendments that enable the government to prosecute its publications.

Such amendments, however, broaden the scope of the criminal activities without properly defining what should be considered a media organization. Such a legislative move endangers not only the activities of online media but also the traditional press. Courts have long respected the line between publishing and communicating leaked information, but judges here focused on the legislative history of the Espionage Act and Congress' decision to exclude the word "publish" from the commonly used § 793. With the expansion of language in § 798, the United States would likely use § 798, once narrowly constructed to apply to particular secret

---

[90] *Espionage Act and the Legal and Constitutional Issues Raised by WikiLeaks: Hearing on H.R. 6506 Before the H. Comm. on the Judiciary*, 111th Cong. 42–43 (2010) (statement of Kenneth L. Wainstein, Partner, O'Melveny & Myers, LLP).

communications and codes, to pursue *both* leaks of "classified information" that present a "transnational threat" and publication of such leaks. Inclusion of the new statutory language in a section of the Espionage Act that explicitly criminalizes publication of restricted information would not only increase the scrutiny of disclosures by WikiLeaks and other Internet-based organizations but also the publications of the very members of the press the courts have protected in the past.

IV. CONCLUSION

Application of the Espionage Act of 1917 has changed since its original passage during World War I. Adapting to fit the need to protect national security during wartime and peacetime, the Act applies to both American citizens and foreign nationals and extends beyond the physical borders of the United States. The advent of computer technology, and perhaps even more importantly, the Internet, has created newer and faster modes of intelligence acquisition, transfer, theft, communication, and publication. Courts have consistently perceived a line between the person who leaks intelligence that threatens national security and the person or institution that publishes the leaked intelligence that threatens national security. The balance between national security and freedom of the press has been respected, but when modern technologies blur the line between leaking and publishing classified data the balance can no longer be so maintained.

The recent WikiLeaks controversy has highlighted the impact of technology on application of the Espionage Act to publication of sensitive government information. As a foreign national, Assange could still be subject to prosecution if the U.S. government could prove he acted as a communicator of dangerous national security information rather than as a traditional member of the press. The multiple technological innovations that enabled the massive transfer and publication of the secret documents make the Assange situation an interesting case study for the future of the Espionage Act in a highly interconnected and networked world. The introduction of the SHIELD Act in Congress, regardless of its future passage, indicates that the legislature is willing to expand

the concept of espionage, potentially including publication even by journalistic institutions, without waiting for decisions from the judiciary regarding whether technologies will mean shifting the fulcrum toward freedom of the press.

Even if Julian Assange is not prosecuted, he could represent a future model of sharing classified information via the Internet, especially when the individual acquiring the secure documents directly posts the information online. In that scenario the individual could be found criminally liable under the Espionage Act, even with the courts' interpretations of a safe haven for the press. Now, web-based technology has blurred the line so that the Supreme Court must be careful to distinguish acquisition of classified data with the role of a publisher—to shed light on the secret dealings of governments to increase transparency for their citizenry. Members of Congress have introduced the SHIELD Act to draw a sharper line, but that bright line comes at the expense of freedom of the press. While Congress is right to address ambiguities in the Espionage Act, the SHIELD Act proposes potentially sweeping changes that signal future targeting of online media organizations not typically regarded as journalistic enterprises. Instead of reacting too quickly to the WikiLeaks release of classified documents, Congress should reevaluate the existing sections of the Espionage Act and fashion language that precisely defines the publication of such information and establishes the limit of criminality once the information has been leaked in order to protect public disclosure. The SHIELD Act offers no such clarification and would instead broaden the type of sensitive information illegal to communicate and would arm the U.S. government with a tool that would restrict both traditional and newer digital media organizations from exposing government actions.

12 N.C. J.L. & TECH. ON. 177, 198
The Espionage Act and WikiLeaks