Criminal Prohibitions on the Publication of Classified Defense Information

Jennifer K. Elsea
Legislative Attorney

June 26, 2012

Congressional Research Service
7-5700
www.crs.gov
R41404

CRS Report for Congress
Prepared for Members and Committees of Congress

Summary

Recent press reports describing classified U.S. operations abroad have led to calls from Congress for an investigation into the source of the leaks, and Attorney General Holder has appointed two special prosecutors to look into the matter. The online publication of classified defense documents and diplomatic cables by the organization WikiLeaks and subsequent reporting by the *New York Times* and other news media had already focused attention on whether such publication violates U.S. criminal law. The suspected source of the WikiLeaks material, Army Private Bradley Manning, has been charged with a number of offenses under the Uniform Code of Military Justice (UCMJ), including aiding the enemy, while a grand jury in Virginia is deciding whether to indict any civilians in connection with the disclosure. A number of other cases involving charges under the Espionage Act demonstrate the Obama Administration's relatively hard-line policy with respect to the prosecution of persons suspected of leaking classified information to the media.

This report identifies some criminal statutes that may apply to the publication of classified defense information, noting that these have been used almost exclusively to prosecute individuals with access to classified information (and a corresponding obligation to protect it) who make it available to foreign agents, or to foreign agents who obtain classified information unlawfully while present in the United States. Leaks of classified information to the press have only rarely been punished as crimes, and we are aware of no case in which a publisher of information obtained through unauthorized disclosure by a government employee has been prosecuted for publishing it. There may be First Amendment implications that would make such a prosecution difficult, not to mention political ramifications based on concerns about government censorship. To the extent that the investigation implicates any foreign nationals whose conduct occurred entirely overseas, any resulting prosecution may carry foreign policy implications related to the exercise of extraterritorial jurisdiction and whether suspected persons may be extradited to the United States under applicable treaty provisions.

This report discusses the statutory prohibitions that may be implicated, including the Espionage Act; the extraterritorial application of such statutes; and the First Amendment implications related to such prosecutions against domestic or foreign media organizations and associated individuals. The report provides a summary of recent legislation relevant to the issue (H.R. 703, S. 315, S. 355, H.R. 1823, H.R. 4310, S.Res. 489) as well as some previous efforts to criminalize the unauthorized disclosure of classified information.

Contents

Contacts

The online publication of classified defense documents and diplomatic cables by the organization WikiLeaks and subsequent reporting by the *New York Times*, *The Guardian* (UK), and *Der Spiegel* (Germany), among others, focused attention on whether such publication violates U.S. criminal law. The suspected source of the material, Army Private Bradley Manning, has been charged with a number of offenses under the Uniform Code of Military Justice (UCMJ). A grand jury has been empanelled in Alexandria, VA, to investigate civilian involvement in the matter,[1] but information regarding the targets of the investigation and the prosecution's theory of the case remains under seal.[2]

Another set of recent newspaper stories reporting on U.S. covert or clandestine operations overseas has led to calls for the appointment of a special prosecutor to investigate executive branch leaks.[3] Attorney General Eric Holder has appointed two U.S. Attorneys to lead FBI investigations into certain possible unauthorized disclosures, but did not reveal which news stories were thought to have reported leaked material.[4] The FBI had reportedly opened investigations into the disclosure of information leading to a news story about the United States' alleged involvement in deploying a computer virus to damage uranium enrichment facilities in Iran[5] and another to look into a report about a foiled terrorist plot.[6] Other news accounts

[1] Scott Shane, *Supporter of Leak Suspect Is Called Before Grand Jury*, NY TIMES, June 16, 2011, at 22. After the Attorney General indicated last December that he had authorized investigators to take "significant" steps with respect to the WikiLeaks case (but declined to elaborate), an attorney for Julian Assange told news reporters that he had learned from Swedish authorities that a grand jury had been empanelled in Alexandria, VA, to investigate the matter. *See* Charlie Savage, *Building Case For Conspiracy By WikiLeaks*, NY TIMES, December 16, 2010, at 1. The attorney reportedly told *Al-Jazeera* in an interview that Julian Assange is at least one target of the investigation. *See Assange attorney: Secret grand jury meeting in Virginia on WikiLeaks*, CNN.COM, December 13, 2010, http://articles.cnn.com/2010-12-13/justice/wikileaks.investigation_1_julian-assange-wikileaks-case-grand-jury?_s=PM:CRIME. However, another of Assange's attorneys refuted the claim, stating Assange's legal team has no concrete evidence that a grand jury is considering charges against Assange. Justin Elliot, *Assange grand jury report "purely speculation"*, WAR ROOM (December 14, 2010), http://www.salon.com/news/politics/war_room/2010/12/14/assange_grand_jury_rumors/index.html. Separate from the grand jury investigation, the U.S. Attorney for the Eastern District of Virginia reportedly subpoenaed records of several persons from the social media network Twitter. *See* Scott Shane and John F. Burns, *Twitter Records in Wikileaks Case are Subpoenaed*, NY TIMES, January 9, 2011, at 1.

[2] Based on a letter accompanying a grand jury subpoena, there is some speculation that federal prosecutors are pursuing a conspiracy theory under the Espionage Act of 1917 as well as laws prohibiting misuse of government computers and misappropriation of government property. *See* Ellen Nakashima and Jerry Markon, *Documents Offer Hints of U.S. Legal Strategy in WikiLeaks Investigation*, WASH. POST, April 29, 2011, at A3. It is believed that a conspiracy theory will permit prosecutors to pursue charges on the basis of activities not subject to First Amendment protection. *See* Shane, *supra* footnote 1 (quoting attorney Abbe D. Lowell).

The subpoena has been posted at http://www.salon.com/news/opinion/glenn_greenwald/2011/06/09/wikileaks/subpoena.pdf. The letter accompanying the subpoena can be viewed at http://www.salon.com/news/opinion/glenn_greenwald/2011/06/09/wikileaks/Ltr.House.pdf. It appears to be a form letter that advises recipients that the grand jury is investigating "possible violations of federal criminal law, but not necessarily limited to conspiracy to" commit violations of 18 U.S.C. §793(g) (espionage), 18 U.S.C. §371 (general conspiracy statute; fraud against the government), 18 U.S.C. §1030 (computer fraud), and 18 U.S.C. §641 (conversion of public property).

[3] *See* Evan Perez, *Holder Puts Top Prosecutors on Leak Probe*, WALL ST. J., June 9, 2012, at A6 (reporting some accusations that the Obama Administration has itself permitted selective leaks of classified information in order to enhance the President's reelection prospects).

[4] *See* Press Release, U.S. Department of Justice Office of Public Affairs, Assignment of U.S. Attorneys to Lead Investigations of Possible Unauthorized Disclosures of Classified Information (June 8, 2012), *available at* http://www.justice.gov/opa/pr/2012/June/12-ag-736.html.

[5] *See* David E. Sanger, *Obama Order Sped Up Wave of Cyberattacks Against Iran*, NY Times, June 1, 2012, at A1, available at http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=1&_r=1&hp. The reporting was based, according to the author, "on interviews over the past 18 months with current and former American, European and Israeli officials involved in the program" and other experts, (continued...)

regarding, for example, the use of unmanned aerial vehicles (also known as drones) for targeted killings abroad[7] have likewise given rise to questions about whether White House officials discuss classified information with journalists, but the scope of the investigations remains unclear.

At this stage in all of these investigations, there is little public information available. Accordingly, the following discussion provides a general overview of the relevant law as it may apply to pertinent allegations reported in the media, assuming them to be true. The discussion should not be interpreted to confirm the truth of any allegations or establish that a particular statute has been violated.

Background

The WikiLeaks Releases

WikiLeaks.org has described itself as a "public service designed to protect whistle-blowers, journalists and activists who have sensitive materials to communicate to the public."[8] Arguing that "[p]rincipled leaking has changed the course of history for the better," it stated that its purpose is to promote transparency in government and fight corporate fraud by publishing information governments or corporations would prefer to keep secret, obtained from sources in person, by means of postal drops, and by using "cutting-edge cryptographic technologies" to receive material electronically.[9] The organization has promised contributors that their anonymity will be protected.

According to press reports, WikiLeaks obtained more than 91,000 secret U.S. military reports related to the war in Afghanistan and posted the majority of them, unredacted, on its website in late July 2010, after first alerting the *New York Times* and two foreign newspapers, the *Guardian* (London) and *Der Spiegel* (Germany), about the pending disclosure.[10] Military officials have charged an Army private, Bradley Manning, for offenses related to the provision of documents to WikiLeaks.[11] Private Manning, a dual U.S.-British citizen, was already in military custody under

(...continued)

none of whom were willing to allow names to be printed because of the classified nature of the program.

[6] *See* Scott Shane and Eric Schmitt, *Qaeda Foiled in Plot to Plant Redesigned Bomb on Plane, U.S. Officials Say*, NY Times, May 8, 2012, at A12.

[7] *See*, *e.g.*, Jo Becker and Scott Shane, *Secret 'Kill List' Proves a Test Of Obama's Principles and Will*, NY TIMES, May 29, 2012, at A1.

[8] http://www.wikileaks.org/wiki/WikiLeaks:About.

[9] *Id*.

[10] The *New York Times* published a series of articles under the headline "The War Logs," which is available online at http://www.nytimes.com/interactive/world/war-logs.html. The *Times* describes the leaked material as an archive covering six years of incident reports and intelligence documents—"usually spare summaries but sometimes detailed narratives"—that "illustrate[s] in mosaic detail why" the military effort in Afghanistan has not weakened the Taliban. C. J. Chivers et al., *The Afghan Struggle: A Secret Archive*, N.Y. TIMES, July 26, 2010, at 1. The German periodical *Der Spiegel* published a series of articles under the topic "Afghanistan Protocol," which is available (in English) online at http://www.spiegel.de/international/world/0,1518,708314,00.html. The *Guardian* (UK) published a series entitled "Afghanistan: The War Logs," which is available online at http://www.guardian.co.uk/world/the-war-logs.

[11] *See* Ed Pilkington, *Bradley Manning May Face Death Penalty*, GUARDIAN (UK), March 3, 2011, *available at* http://www.guardian.co.uk/world/2011/mar/03/bradley-manning-may-face-death-penalty (reporting that 22 new charges, including aiding the enemy, were added to the original twelve specifications).

suspicion of having provided WikiLeaks with video footage of an airstrike that resulted in the deaths of civilians.[12] The most serious charge, aiding the enemy in violation of UCMJ Article 104,[13] is a capital offense, but prosecutors have reportedly said they do not intend to seek the death penalty.[14] It is also one of two offenses under the UCMJ that apply to "any person," rather than "any person subject to [chapter 47 of title 10, U.S. Code]" as defined in UCMJ article 2,[15] which raises the possibility that civilians who are not connected with the military could be similarly charged. There has been no suggestion that court-martial of any civilians has been considered in connection with the disclosure, and such a prosecution would likely be subject to constitutional challenge.

U.S. officials have condemned the leaks, predicting that the information disclosed could lead to the loss of lives of U.S. soldiers in Afghanistan and Afghan citizens who have provided them assistance.[16] Defense Secretary Robert M. Gates informed members of Congress that a preliminary review of the disclosed information by the Defense Department found that no sensitive information related to intelligence sources or methods was made public, but reiterated that the release of Afghan informants' names could have "potentially dramatic and grievously harmful consequences."[17] WikiLeaks subsequently released some 400,000 documents related to the war in Iraq,[18] this time with names of informants apparently redacted.[19]

In late November 2010, WikiLeaks began publishing what the *New York Time*s calls a "mammoth cache of a quarter-million confidential American diplomatic cables," dated for the most part from 2008-2010.[20] WikiLeaks.org posted 220 cables on November 28, 2010, as a first installment, some of which were redacted to protect diplomatic sources. The most recent documents in the collection are reportedly dated February 2010,[21] but some of them apparently go back several decades.[22]

---

[12] *Military airstrike video leak suspect in solitary confinement*, CNN.com, August 1, 2010, *available at* http://www.cnn.com/2010/POLITICS/07/31/wikileaks.manning/index.html.

[13] 10 U.S.C. §904.

[14] *See* Jim Miklaszewski and Courtney Kube, *Manning faces new charges, possible death penalty*, MSNBC.com, May 3, 2011, *available at* http://www.msnbc.msn.com/id/41876046/ns/us_news-security/.

[15] 10 U.S.C. §802. The only UCMJ offense that applies more broadly than to persons subject to UCMJ jurisdiction under Article 2 is spying, Article 106 (10 U.S.C. §106), which applies to "any person ... in time of war."

[16] Admiral Michael Mullen, Chairman of the Joint Chiefs of Staff, on *Meet the Press*, August 1, 2010, transcript available at http://www.msnbc.msn.com/id/38487969/ns/meet_the_press-transcripts/.

[17] *See* Elisabeth Bumiller, *Gates Found Cost of Leaks Was Limited*, NY TIMES, October 17, 2010 (quoting letter to Senator Levin from Secretary Gates).

[18] *See The Iraq Archive: The Strands of a War*, NY TIMES, at http://www.nytimes.com/2010/10/23/world/middleeast/23intro.html?_r=1.

[19] *See* Anna Mulrine, Wikileaks *Iraq Documents not as Damaging as Pentagon Feared—Yet*, CHRISTIAN SCIENCE MONITOR, October 25, 2010. The *New York Times* has stated it redacted names prior to publishing the leaked materials. *See The Iraq Archive*, *supra* footnote 18.

[20] *State's Secrets*, NY TIMES (online edition), November 29, 2010, http://www.nytimes.com/interactive/world/statessecrets.html. According to the *Guardian*, the fact that most of the cables are dated from 2008 to 2009 is explained by the increase in the number of U.S. embassies linked to the military's secure computer network, SIPRNet, over the past decade. *See The US embassy cables*, GUARDIAN (UK), http://www.guardian.co.uk/news/datablog/2010/nov/29/wikileaks-cables-data.

[21] Scott Shane and Andrew W. Lehren, *Cables Obtained by WikiLeaks Shine Light Into Secret Diplomatic Channels*, NY TIMES.

[22] The *Guardian* states that the earliest of the cables is from 1966. *See The US embassy cables*, *supra* footnote 20.

The United States government was aware of the impending disclosure, although not apparently directly informed by the web-based anti-secrecy organization (or given access to the documents to be released). WikiLeaks Editor in Chief Julian Assange, in a letter sent to the U.S. ambassador to the UK, Louis Susman, offered to consider any U.S. requests to protect specific information that the government believes could, if published, put any individuals at significant risk of harm.[23] The State Department Legal Adviser responded in a letter to Mr. Assange's attorney that the publication of classified materials violates U.S. law, that the United States will not negotiate with WikiLeaks with respect to the publication of illegally obtained classified documents, and that WikiLeaks should cease these activities and return all documents, as well as delete any classified U.S. government material in its possession from its databases.[24] Mr. Assange responded by accusing the United States of adopting a confrontational stance and indicating an intent to continue publishing the materials, subject to the checks WikiLeaks and its media partners planned to implement to reduce any risk to individuals.[25]

After learning the classified cables were to be published, the Defense Department notified the U.S. Senate and House Armed Services Committees in general terms about what to expect.[26] Assistant Secretary for Legislative Affairs Elizabeth King explained that "State Department cables by their nature contain everyday analysis and candid assessments that any government engages in as part of effective foreign relations," and predicted that the publication of the classified cables, which she described as intended to "wreak havoc and destabilize global security," could potentially jeopardize lives.[27] State Department spokesman Philip J. Crowley told *Bloomberg* that the State Department was "assessing the possible impact on our on-going diplomatic activity and notifying both Congress and other governments what may occur."[28] The White House issued a statement condemning the activities of WikiLeaks[29] and ordered all agencies to conduct reviews of their information security policies and programs.[30]

---

[23] Letter to Ambassador Susman, November 26, 2010, *available at* http://documents.nytimes.com/letters-between-wikileaks-and-gov.

[24] Letter from State Department Legal Adviser Harold Hongju Koh to Jennifer Robinson, November 27, 2010, *available at* http://documents.nytimes.com/letters-between-wikileaks-and-gov.

[25] Letter to Ambassador Susman, November 28, 2010, *available at* http://documents.nytimes.com/letters-between-wikileaks-and-gov.

[26] Tony Capaccio, *Pentagon Alerts House, Senate Panels to New Classified WikiLeaks Release*, BLOOMBERG, November 24, 2010, http://www.bloomberg.com/news/2010-11-24/pentagon-warns-house-senate-defense-panels-of-more-wikileaks-documents.html.

[27] *Id.*

[28] *Id.*

[29] White House, Statement of the Press Secretary, November 28, 2010, at http://www.whitehouse.gov/the-press-office/2010/11/28/statement-press-secretary. The statement reads in full:

> We anticipate the release of what are claimed to be several hundred thousand classified State department cables on Sunday night that detail private diplomatic discussions with foreign governments. By its very nature, field reporting to Washington is candid and often incomplete information. It is not an expression of policy, nor does it always shape final policy decisions. Nevertheless, these cables could compromise private discussions with foreign governments and opposition leaders, and when the substance of private conversations is printed on the front pages of newspapers across the world, it can deeply impact not only US foreign policy interests, but those of our allies and friends around the world. To be clear—such disclosures put at risk our diplomats, intelligence professionals, and people around the world who come to the United States for assistance in promoting democracy and open government. These documents also may include named individuals who in many cases live and work under oppressive regimes and who are trying to create more open and free societies. President Obama supports responsible, accountable, and open government at home and around the world, but this reckless and dangerous action runs

(continued...)

As of early January 2011, about 1% of the cables had been published, with WikiLeaks.org posting only those cables that had already been released by the newspapers, as redacted by the newspapers.[31] The State Department warned human rights activists, foreign government officials, and businesspeople who are identified in the diplomatic cables that they may be at risk, although their names had not been published thus far, and relocated a few of them for their safety.[32] The cables continued to be released at an apparently steady rate,[33] until it was discovered in late August, 2011, that the entire unredacted file had been published on the web along with the password needed to access the data.[34] WikiLeaks then began publishing the remaining documents at a much faster pace, so that all of the more than 250,000 diplomatic cables are accessible without redactions on the Internet.[35]

Other Leaks Prosecutions

The Obama Administration is taking a relatively hard-line stance with respect to those suspected of leaking classified information to the press, with six prosecutions currently under way or completed (including Bradley Manning).[36] A former National Security Agency (NSA) official, Thomas A. Drake, recently agreed to plead guilty to exceeding authorized use of a government computer in violation of 18 U.S.C. Section 1030(a)(2)(B) (a misdemeanor), after the government dropped more serious charges under the Espionage Act, among other offenses.[37] Mr. Drake was initially investigated beginning in 2007 in connection with the *New York Times*' revelations regarding the Bush Administration's warrantless surveillance program, but was eventually charged in connection with providing classified information that revealed alleged NSA mismanagement to the *Baltimore Sun*.[38] The prosecution eventually dropped most of the charges

(...continued)

> counter to that goal. By releasing stolen and classified documents, Wikileaks has put at risk not only the cause of human rights but also the lives and work of these individuals. We condemn in the strongest terms the unauthorized disclosure of classified documents and sensitive national security information.

[30] Memorandum from Jacob J. Lew, Director, Office of Management and Budget to Heads of Executive Departments and Agencies (November 28, 2010), at http://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-06.pdf. For other White House responses to the WikiLeaks disclosures, see FACT SHEET: U.S. Government Mitigation Efforts in Light of the Recent Unlawful Disclosure of Classified Information (December 1, 2010), at http://www.whitehouse.gov/search/site/classified%20information.

[31] *See* Mark Landler and Scott Shane, *U.S. Sends Warning to People Named in Cable Leaks*, N.Y. TIMES, January6, 2011.

[32] *Id*.

[33] For information related to the content of the cables, see *Wikileaked: Inside the State Department's Secret Cables*, FOREIGN POL'Y, http://wikileaks.foreignpolicy.com/; *The US embassy cables*, *supra* footnote 20.

[34] *See* Kim Zetter, *U.S. Sources Exposed as Unredacted State Department Cables Are Unleashed Online*, THREAT LEVEL (September 1, 2011, 3:22 PM), http://www.wired.com/threatlevel/2011/09/wikileaks-unredacted-cables/.

[35] *See* Scott Shane, *Spread of Leaked Cables on Web Prompts Dispute*, NY Times, September 1, 2011, *available at* http://www.nytimes.com/2011/09/02/us/02wikileaks.html?_r=1.

[36] *See* Scott Shane, *Ex-N.S.A. Official Takes Plea Deal*, NY TIMES, June 10, 2011, at A1, *available at* http://www.nytimes.com/2011/06/10/us/10leak.html?_r=1.

[37] *See* Ellen Nakashima, *Ex-NSA official Thomas Drake to plead guilty to misdemeanor*, WASH. POST, June 9, 2011, at http://www.washingtonpost.com/national/national-security/ex-nsa-manager-has-reportedly-twice-rejected-plea-bargains-in-espionage-act-case/2011/06/09/AG89ZHNH_story.html.

[38] *See* Jane Mayer, *The Secret Sharer*, New Yorker, May 23, 2011, http://www.newyorker.com/reporting/2011/05/23/110523fa_fact_mayer.

after the judge ruled that the government's proposed substitutions for documentary evidence it sought to introduce would not provide an adequate opportunity for the defendant to present his case.[39] After calling the government's treatment of the defendant in the case "unconscionable" and declining to impose a fine, the court sentenced Mr. Drake to one year probation and 240 hours of community service.[40]

A guilty plea was also secured in a case against an FBI contract linguist accused of providing secret documents to a blogger.[41] The defendant, Shamai Kedem Leibowitz, was sentenced to 20 months in prison for violation of 18 U.S.C. Section 798 by passing five documents classified at the "secret" level in relation to communications intelligence.[42]

The Obama Administration is seeking to compel *New York Times* reporter James Risen to testify at the trial of former CIA officer Jeffrey Sterling, who is accused of providing classified information to Mr. Risen that formed the basis of part of a book.[43] The judge ruled, however, that Mr. Risen need only testify about certain non-privileged information and need not identify the source of the material in question.[44] The government asked the court to reconsider the ruling, arguing that the reporter's testimony is "qualitatively different" from the circumstantial evidence the judge thought would suffice to establish the same facts,[45] but the court declined to reconsider. The government has filed an appeal of the order at the Court of Appeals for the Fourth Circuit.[46] The government is also appealing an order striking two of its primary witnesses for failure to produce information about them to the defense in a timely manner.[47]

Another ongoing prosecution involved a former State Department contractor who was indicted in 2010 for disclosing national defense information to a news organization, believed to be Fox News, related to intelligence regarding North Korea's nuclear weapons program.[48] The contractor, Stephen Kim, was at the time of the disclosure a senior adviser for intelligence detailed to the State Department's arms control compliance bureau.[49] The court denied the defendant's motions

[39] United States v. Drake, Crim. No. 10 CR 00181 RDB (N.D. Md.) (Government Motion to Dismiss the Indictment at the Time of Sentencing) (filed June 10, 2011), *available at* http://www.fas.org/sgp/jud/drake/061011-dismiss.pdf.

[40] *See* Steven Aftergood, *Handling of Drake Leak Case was "Unconscionable," Court Said*, SECRECY NEWS (July 29, 2011), http://www.fas.org/blog/secrecy/2011/07/drake_transcript.html.

[41] *See* Press Release, Department of Justice, Former FBI Contract Linguist Pleads Guilty to Leaking Classified Information to Blogger (December 17, 2009), *available at* http://www.justice.gov/opa/pr/2009/December/09-nsd-1361.html.

[42] *Id*.

[43] Jeffrey Sterling was indicted for several counts of violating the Espionage Act (disclosure and retention of national defense information) as well as mail fraud, conversion of government property, and obstruction of justice. The indictment is available at http://www.fas.org/sgp/jud/sterling/indict.pdf.

[44] Steven Aftergood, *Reporter Risen Will Not Have to Identify Source in Leak Trial*, SECRECY NEWS (August 1, 2011), http://www.fas.org/blog/secrecy/2011/08/risen_off_hook.html. For an overview of the law regarding the reporter's privilege, see CRS Report RL34193, *Journalists' Privilege: Overview of the Law and Legislation in Recent Congresses*, by Kathleen Ann Ruane.

[45] *See* Government's Motion for Clarification and Reconsideration, United States v. Sterling, No. 1:10cr485 (E.D. Va. August 24, 2011), *available at* http://www.fas.org/sgp/jud/sterling/082411-recon.pdf.

[46] United States v. Sterling, No. 11-5028 (4th Cir. October 19, 2011)(filed).

[47] *Id*.

[48] *See* Spencer S. Hsu, *State Dept. contractor charged in leak to news organization*, WASH. POST, August 28, 2010.

[49] *Id*.

to dismiss the espionage charges based on the Constitution's Treason Clause as well as the First and Fifth Amendments.[50]

A former CIA officer, John Kiriakou, is the latest person to be charged for the unauthorized disclosure of classified information to a journalist. Because the disclosures are alleged to have included the identities of covert CIA employees, he has also been charged under the Intelligence Identities Protection Act.[51] His trial is scheduled to begin in November.

The publication of the leaked documents by WikiLeaks and the subsequent reporting of information contained therein, as well as other publications of "leaked" classified information, raise questions with respect to the possibility of bringing criminal charges for the dissemination of materials by media organizations following an unauthorized disclosure, in particular when done by non-U.S. nationals overseas. This report discusses the statutory prohibitions that may be implicated; the extraterritorial application of such statutes; and the First Amendment implications related to such prosecutions against domestic or foreign media organizations and associated individuals.

Statutory Protection of Classified Information

While there is no one statute that criminalizes the unauthorized disclosure of any classified information, a patchwork of statutes exists to protect information depending upon its nature, the identity of the discloser and of those to whom it was disclosed, and the means by which it was obtained. It seems likely that most of the information disclosed by WikiLeaks that was obtained from Department of Defense databases falls under the general rubric of information related to the national defense. The diplomatic cables obtained from State Department channels may also contain information relating to the national defense and thus be covered under the Espionage Act, but otherwise their disclosure by persons who are not government employees does not appear to be directly proscribed.[52] It is possible that some of the government information disclosed in any of the releases does not fall under the express protection of any statute, despite its classified status.

The Espionage Act

National defense information in general is protected by the Espionage Act,[53] 18 U.S.C. Sections 793–798, while other types of relevant information are covered elsewhere. Some provisions apply only to government employees or others who have authorized access to sensitive government information,[54] but many apply to all persons. 18 U.S.C. Section 793 prohibits the gathering, transmitting, or receipt of defense information with the intent or reason to believe the information

[50] United States v. Kim, 808 F. Supp. 2d 44 (D.D.C. 2011).

[51] 50 U.S.C. §§421-426. For more information about this statute, see CRS Report RS21636, *Intelligence Identities Protection Act*, by Jennifer K. Elsea.

[52] *See* 18 U.S.C. §952 (prohibiting the disclosure or publication of certain diplomatic material obtained "by virtue of … employment by the United States").

[53] Act of October 6, 1917, ch. 106, §10(i), 40 Stat. 422.

[54] *E.g.*, 18 U.S.C. §§952 (prohibiting disclosure of diplomatic codes and correspondence), 1924 (unauthorized removal and retention of classified documents or material); 50 U.S.C. §783 (unauthorized disclosure of classified information to an agent of a foreign government, unauthorized receipt by foreign government official).

will be used against the United States or to the benefit of a foreign nation. Violators are subject to a fine or up to 10 years' imprisonment, or both,[55] as are those who conspire to violate the statute.[56] Persons who possess defense information that they have reason to know could be used to harm the national security, whether the access is authorized or unauthorized, and who disclose that information to any person not entitled to receive it, or who fail to surrender the information to an officer of the United States, are subject to the same penalty.[57] Although it is not necessary that the information be classified by a government agency, the courts seem to give deference to the executive determination of what constitutes "defense information."[58] Information that is made

[55] 18 U.S.C. §793(a)-(c) provides:

> (a) Whoever, 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, goes upon, enters, flies over, or otherwise obtains information concerning any vessel, aircraft, work of defense, [etc.], or any prohibited place so designated by the President by proclamation in time of war or in case of national emergency in which anything for the use of the Army, Navy, or Air Force is being prepared or constructed or stored, information as to which prohibited place the President has determined would be prejudicial to the national defense; or
>
> (b) Whoever, for the purpose aforesaid, and with like intent or reason to believe, copies, takes, makes, or obtains, or attempts to copy, take, make, or obtain any sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, document, writing, or note of anything connected with the national defense; or
>
> (c) Whoever, for the purpose aforesaid, receives or obtains or agrees or attempts to receive or obtain from any person, or from any source whatever, any [protected thing] connected with the national defense, knowing or having reason to believe ... that it has been or will be obtained, taken, made, or disposed of by any person contrary to the provisions of this chapter [18 U.S.C. §§792 *et seq*.]....

[56] 18 U.S.C. §793(g) provides

> If two or more persons conspire to violate any of the foregoing provisions of this section, and one or more of such persons do any act to effect the object of the conspiracy, each of the parties to such conspiracy shall be subject to the punishment provided for the offense which is the object of such conspiracy.

[57] 18 U.S.C. §793(e) provides

> Whoever having unauthorized possession of, access to, or control over any document [or other protected thing], or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits ... to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it; … Shall be fined under this title or imprisoned not more than ten years, or both.

§793(d) is identical to §794(e), except that it applies to persons with authorized access to the information at issue, in which case it is only an offense to retain or fail to turn the information over to a government official if there was a demand for its return.

§793(f) likewise applies only to those with authorized access to the covered materials, punishing those who

> (1) through gross negligence permits the same to be removed from its proper place of custody or delivered to anyone in violation of his trust, or to be lost, stolen, abstracted, or destroyed, or
>
> (2) having knowledge that the same has been illegally removed from its proper place of custody or delivered to anyone in violation of its trust, or lost, or stolen, abstracted, or destroyed, and fails to make prompt report of such loss, theft, abstraction, or destruction to his superior officer.

[58] The government must demonstrate that disclosure of the information is at least "potentially damaging" to the United States or advantageous to a foreign government. *See* United States v. Morison, 844 F.2d 1057, 1072 (4th Cir.), *cert. denied*, 488 U.S. (1988)(upholding conviction under 18 U.S.C. §793 for delivery of classified photographs to publisher). Whether the information is "related to the national defense" under this meaning is a question of fact for the jury to decide. *Id*. at 1073.

available by the government to the public is not covered under the prohibition, however, because public availability of such information negates the bad-faith intent requirement.[59] On the other hand, classified documents remain within the ambit of the statute even if information contained therein is made public by an unauthorized leak.[60]

18 U.S.C. Section 794 (aiding foreign governments or communicating information to an enemy in time of war) covers "classic spying" cases,[61] providing for imprisonment for any term of years or life, or under certain circumstances, the death penalty.[62] The provision penalizes anyone who transmits defense information to a foreign government (or foreign political or military party) with the intent or reason to believe it will be used against the United States. It also prohibits attempts to elicit information related to the public defense "which might be useful to the enemy."[63] The death penalty is available only upon a finding that the offense resulted in the death of a covert agent or directly concerns nuclear weapons or other particularly sensitive types of information. The death penalty is also available under Section 794 for violators who gather, transmit or publish information related to military plans or operations and the like during time of war, with the intent that the information reach the enemy.[64] These penalties are available to punish any person who

[59] Gorin v. United States, 312, U.S. 9, 27-28 (1941) ("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.").

[60] United States v. Squillacote, 221 F.3d 542, 578 (4th Cir. 2000).

[61] *Morison*, 844 F.2d at 1064-65 (explaining that critical element distinguishing §794 from §793 is the requirement that disclosure be made to an agent of a foreign government rather than anyone not entitled to receive it).

[62] §794. Gathering or delivering defense information to aid foreign government

> (a) Whoever, with intent or reason to believe that it is to be used to the injury of the United States or to the advantage of a foreign nation, communicates, delivers, or transmits ... to any foreign government, or to any faction or party or military or naval force within a foreign country, whether recognized or unrecognized by the United States, or to any representative, officer, agent, employee, subject, or citizen thereof, either directly or indirectly, any document [or other protected thing], or information relating to the national defense, shall be punished by death or by imprisonment for any term of years or for life, except that the sentence of death shall not be imposed unless the jury or ... the court, further finds that the offense resulted in the identification by a foreign power (as defined in section 101(a) of the Foreign Intelligence Surveillance Act of 1978 [50 U.C.S. §1801(a)]) of an individual acting as an agent of the United States and consequently in the death of that individual, or directly concerned nuclear weaponry, military spacecraft or satellites, early warning systems, or other means of defense or retaliation against large-scale attack; war plans; communications intelligence or cryptographic information; or any other major weapons system or major element of defense strategy.

[63] §794(b) provides:

> (b) Whoever, in time of war, with intent that the same shall be communicated to the enemy, collects, records, publishes, or communicates, or attempts to elicit any information with respect to the movement, numbers, description, condition, or disposition of any of the Armed Forces, ships, aircraft, or war materials of the United States, or with respect to the plans or conduct, or supposed plans or conduct of any naval or military operations, or with respect to any works or measures undertaken for or connected with, or intended for the fortification or defense of any place, or any other information relating to the public defense, which might be useful to the enemy, shall be punished by death or by imprisonment for any term of years or for life....

[64] During time of war, any individual who communicates intelligence or any other information to the enemy may be prosecuted by the military for aiding the enemy under Article 104 of the Uniform Code of Military Justice (UCMJ), and if convicted, punished by "death or such other punishment as a court-martial or military commission may direct." 10 U.S.C. §904.

participates in a conspiracy to violate the statute. Offenders are also subject to forfeiture of any ill-gotten gains and property used to facilitate the offense.[65]

The unauthorized creation, publication, sale or transfer of photographs or sketches of vital defense installations or equipment as designated by the President is prohibited by 18 U.S.C. Sections 795 and 797.[66] Violators are subject to fine or imprisonment for not more than one year, or both.

The knowing and willful disclosure of certain classified information is punishable under 18 U.S.C. Section 798 by fine and/or imprisonment for not more than 10 years.[67] To incur a penalty, the disclosure must be prejudicial to the safety or interests of the United States or work to the benefit of any foreign government and to the detriment of the United States. The provision applies only to information related to cryptographic systems or communications intelligence that is specially designated by a U.S. government agency for "limited or restricted dissemination or distribution."[68]

---

[65] 18 U.S.C. §794(d). Proceeds go to the Crime Victims Fund.

[66] §795. Photographing and sketching defense installations

> (a) Whenever, in the interests of national defense, the President defines certain vital military and naval installations or equipment as requiring protection against the general dissemination of information relative thereto, it shall be unlawful to make any photograph, sketch, picture, drawing, map, or graphical representation of such vital military and naval installations or equipment without first obtaining permission of the commanding officer of the military or naval post, camp, or station, or naval vessels, military and naval aircraft, and any separate military or naval command concerned, or higher authority, and promptly submitting the product obtained to such commanding officer or higher authority for censorship or such other action as he may deem necessary....

§797. Publication and sale of photographs of defense installations

> On and after thirty days from the date upon which the President defines any vital military or naval installation or equipment as being within the category contemplated under section 795 of this title [18], whoever reproduces, publishes, sells, or gives away any photograph, sketch, picture, drawing, map, or graphical representation of the vital military or naval installations or equipment so defined, without first obtaining permission of the commanding officer ... or higher authority, unless such photograph, sketch, picture, drawing, map, or graphical representation has clearly indicated thereon that it has been censored by the proper military or naval authority, shall be fined under this title or imprisoned not more than one year, or both.

[67] §798. Disclosure of classified information

> (a) 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 the United States any classified information—
>
> (1) concerning the nature, preparation, or use of any code, cipher, or cryptographic system of the United States or any foreign government; or
>
> (2) concerning the design, construction, use, maintenance, or repair of any device, apparatus, or appliance used or prepared or planned for use by the United States or any foreign government for cryptographic or communication intelligence purposes; or
>
> (3) concerning the communication intelligence activities of the United States or any foreign government; or
>
> (4) obtained by the processes of communication intelligence from the communications of any foreign government, knowing the same to have been obtained by such processes—
>
> Shall be fined … or imprisoned not more than ten years, or both.

[68] 18 U.S.C. §798(b).

Members of the military[69] who commit espionage, defined similarly to the conduct prohibited in 18 U.S.C. Section 794, may be tried by court-martial for violating Article 106a of the Uniform Code of Military Justice (UCMJ),[70] and sentenced to death if certain aggravating factors are found by unanimous determination of the panel.[71] Unlike offenses under Section 794, Article 106a offenses need not have resulted in the death of a covert agent or involve military operations during war to incur the death penalty. One of the aggravating factors enabling the imposition of the death penalty under Article 106a is that "[t]he accused has been convicted of another offense involving espionage or treason for which either a sentence of death or imprisonment for life was authorized by statute."

However, the government is not limited to charging the offense of espionage under Article 106a, discussed above. Members could also be tried by court-martial for violations of Article 92, failure to obey order or regulation,[72] Article 104, aiding the enemy,[73] or under the general article, Article 134.[74] Article 134 offenses include "all disorders and neglects to the prejudice of good order and discipline in the armed forces, all conduct of a nature to bring discredit upon the armed forces, and crimes and offenses not capital"[75] that are not enumerated elsewhere in the UCMJ. Specifically, clause 3 of Article 134 (crimes and offenses not capital) may be utilized to try a member of the military for a violation of applicable federal law, such as 18 U.S.C. Section 1030(a) discussed below, not addressed by the UCMJ.

---

[69] Persons subject to the UCMJ include members of regular components of the Armed Forces, cadets and midshipmen, members of reserve components while on training, members of the National Guard when in federal service, members of certain organizations when assigned to and serving the Armed Forces, prisoners of war, persons accompanying the Armed Forces in the field in time of war or a "contingency operation," and certain others with military status. 10 U.S.C. §802.

[70] 10 U.S.C. §906a(a) provides

Art. 106a. Espionage

> (a)(1) Any person subject to [the UCMJ, chapter 47 of title 10, U.S.C.] who, with intent or reason to believe that it is to be used to the injury of the United States or to the advantage of a foreign nation, communicates, delivers, or transmits, or attempts to communicate, deliver, or transmit, to any entity described in paragraph (2), either directly or indirectly, anything described in paragraph (3) shall be punished as a court-martial may direct, except that if the accused is found guilty of an offense that directly concerns (A) nuclear weaponry, military spacecraft or satellites, early warning systems, or other means of defense or retaliation against large scale attack, (B) war plans, (C) communications intelligence or cryptographic information, or (D) any other major weapons system or major element of defense strategy, the accused shall be punished by death or such other punishment as a court-martial may direct.
>
> (2) An entity referred to in paragraph (1) is—
>
> > (A) a foreign government;
> >
> > (B) a faction or party or military or naval force within a foreign country, whether recognized or unrecognized by the United States; or
> >
> > (C) a representative, officer, agent, employee, subject, or citizen of such a government, faction, party, or force.
>
> (3) A thing referred to in paragraph (1) is a document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, note, instrument, appliance, or information relating to the national defense.

[71] 10 U.S.C. §906a(b)-(c).

[72] 10 U.S.C. §892.

[73] 10 U.S.C. §904.

[74] 10 U.S.C. §934.

[75] *Id*.

Other Statutes

18 U.S.C. Section 1030(a)(1) punishes the willful retention, communication, or transmission, etc., of classified information retrieved by means of knowingly accessing a computer without (or in excess of) authorization, with reason to believe that such information "could be used to the injury of the United States, or to the advantage of any foreign nation." Receipt of information procured in violation of the statute is not addressed, but depending on the specific facts surrounding the unauthorized access, criminal culpability might be asserted against persons who did not themselves access a government computer as conspirators, aiders and abettors, or accessories after the fact.[76] The provision imposes a fine or imprisonment for not more than 10 years, or both, in the case of a first offense or attempted violation. Repeat offenses or attempts can incur a prison sentence of up to 20 years.

18 U.S.C. Section 641 punishes the theft or conversion of government property or records for one's own use or the use of another. While this section does not explicitly prohibit disclosure of classified information, it has been used to prosecute "leakers."[77] Violators may be fined, imprisoned for not more than 10 years, or both, unless the value of the property does not exceed the sum of $100, in which case the maximum prison term is one year. The statute also covers knowing receipt or retention of stolen or converted property with the intent to convert it to the recipient's own use. It does not appear to have been used to prosecute any recipients of classified information even where the original discloser was charged under the statute.

50 U.S.C. Section 421 provides for the protection of information concerning the identity of covert intelligence agents.[78] It generally covers persons authorized to know the identity of such agents or who learn the identify of covert agents as a result of their general access to classified information,[79] but can also apply to a person who learns of the identity of a covert agent through a

[76] Charges of conspiracy or aiding and abetting may be available with respect to any of the statutes summarized here, even if the statutes themselves do not mention such charges under the general conspiracy statute, 18 U.S.C. §371, or for aiding and abetting and the like under 18 U.S.C. §§2-4, unless otherwise made inapplicable. Some of the provisions that apply only to government employees or persons with authorized access to classified information may therefore be applied to a broader set of potential violators. For more information about conspiracy law, see CRS Report R41223, *Federal Conspiracy Law: A Brief Overview*, by Charles Doyle.

[77] *See* United States v. Morison, 844 F.2d 1057 (4th Cir. 1988)(photographs and reports were tangible property of the government); United States v. Fowler, 932 F.2d 306 (4th Cir. 1991)("information is a species of property and a thing of value" such that "conversion and conveyance of governmental information can violate §641," citing United States v. Jeter, 775 F.2d 670, 680-82 (6th Cir. 1985)); United States v. Girard, 601 F.2d 69, 70-71 (2d Cir. 1979). The statute was used to prosecute a DEA official for leaking unclassified but restricted documents pertinent to an agency investigation. *See* Dan Eggen, *If the Secret's Spilled, Calling Leaker to Account Isn't Easy*, WASH. POST, October 3, 2003, at A5 (reporting prosecution of Jonathan Randel under conversion statute for leaking government documents to journalist).

[78] The Intelligence Identities and Protection Act of 1982, codified at 50 U.S.C. §§421-26. For more information, see CRS Report RS21636, *Intelligence Identities Protection Act*, by Jennifer K. Elsea. The term "covert agent" is defined to include a non-U.S. citizen "whose past or present intelligence relationship to the United States is classified information and who is a present or former agent of, or a present or former informant or source of operational assistance to, an intelligence agency." 50 U.S.C. §426(4)(c). "Intelligence agency" is defined to include a "foreign intelligence component of the Department of Defense"; informant means "any individual who furnishes information to an intelligence agency in the course of a confidential relationship." 50 U.S.C. §426(5-6). The definitions suggest that the act is intended to protect the identities of persons who provide intelligence information directly to a military counterintelligence unit, but perhaps they can be read to cover those who provide information to military personnel carrying out other functions who provide situation reports intended to reach an intelligence component. In any event, the extraterritorial application of the statute is limited to U.S. citizens and permanent resident aliens. 50 U.S.C. §424.

[79] Persons with direct access to information regarding the identities are subject to a prison term of not more than 10 years, while those who learn the identities through general access to classified information are subject to a term not (continued...)

"pattern of activities intended to identify and expose covert agents" and discloses the identity to any individual not authorized access to classified information, with reason to believe that such activities would impair U.S. foreign intelligence efforts. This crime is subject to a fine or imprisonment for a term of not more than three years. To be convicted, a violator must have knowledge that the information identifies a covert agent whose identity the United States is taking affirmative measures to conceal. To date, there have been no reported cases interpreting the statute, but it did result in one conviction pursuant to a guilty plea.[80]

18 U.S.C. Section 1924 prohibits the unauthorized removal of classified material by government employees, contractors, and consultants who come into possession of the material by virtue of their employment by the government.[81] The provision imposes a fine of up to $1,000 and a prison term up to one year for offenders who knowingly remove material classified pursuant to government regulations concerning the national defense or foreign relations of the United States, with the intent of retaining the materials at an unauthorized location.[82]

There appears to be no statute that generally proscribes the acquisition or publication of diplomatic cables, although government employees who disclose such information without proper authority may be subject to prosecution. 18 U.S.C. Section 952 punishes employees of the United States who, without authorization, willfully publish or furnish to another any official diplomatic code or material prepared in such a code, by imposing a fine, a prison sentence (up to 10 years), or both. The same punishment applies for materials "obtained while in the process of transmission between any foreign government and its diplomatic mission in the United States,"[83] but not, apparently, materials obtained during transmission from U.S. diplomatic missions abroad to the State Department or vice versa (unless the material was or purports to have been prepared using an official diplomatic code—it is unclear whether messages that are encrypted for transmission are covered). The removal of classified material concerning foreign relations with the intent to store them at an unauthorized location is a misdemeanor under 18 U.S.C. Section 1924, which also applies only to U.S. government employees.

(...continued)

greater than five years. 50 U.S.C. §421. Charges of conspiracy, aiding and abetting, or misprision of felony are not available in connection with the offense, except in the case of a person who engaged in a pattern of activities to disclose the identities of covert agents or persons with authorized access to classified information. 50 U.S.C. §422(b).

[80] *See* Richard B. Schmitt, *Rare Statute Figures in Rove Case*, LA TIMES, July 15, 2005, at A15 (reporting 1985 conviction of Sharon Scranage, a clerk for the CIA in Ghana, for disclosing identities of covert agents).

[81] 18 U.C.S. §1924 provides

> (a) Whoever, being an officer, employee, contractor, or consultant of the United States, and, by virtue of his office, employment, position, or contract, becomes possessed of documents or materials containing classified information of the United States, knowingly removes such documents or materials without authority and with the intent to retain such documents or materials at an unauthorized location shall be fined not more than $ 1,000, or imprisoned for not more than one year, or both.
>
> (b) For purposes of this section, the provision of documents and materials to the Congress shall not constitute an offense under subsection (a).
>
> (c) In this section, the term "classified information of the United States" means information originated, owned, or possessed by the United States Government concerning the national defense or foreign relations of the United States that has been determined pursuant to law or Executive order to require protection against unauthorized disclosure in the interests of national security.

[82] *Id*.

[83] 18 U.S.C. §952.

50 U.S.C. Section 783 penalizes government officers or employees who, without proper authority, communicate classified information to a person whom the employee has reason to suspect is an agent or representative of a foreign government.[84] It is also unlawful for the representative or agent of the foreign government to receive classified information.[85] Violation of either of these provisions is punishable by a fine of up to $10,000 or imprisonment for not more than 10 years.[86] Violators are thereafter prohibited from holding federal public office.[87] Violators must forfeit all property derived directly or indirectly from the offense and any property that was used or intended to be used to facilitate the violation.[88]

Analysis

In light of the foregoing, it seems that there is ample statutory authority for prosecuting individuals who elicit or disseminate many of the documents at issue, as long as the intent element can be satisfied and potential damage to national security can be demonstrated.[89] There is some authority, however, for interpreting 18 U.S.C. Section 793, which prohibits the communication, transmission, or delivery of protected information to anyone not entitled to possess it, to exclude the "publication" of material by the media.[90] Publication is not expressly

[84] 50 U.S.C. §783(a) provides:

> Communication of classified information by Government officer or employee. It shall be unlawful for any officer or employee of the United States or of any department or agency thereof, or of any corporation the stock of which is owned in whole or in major part by the United States or any department or agency thereof, to communicate in any manner or by any means, to any other person whom such officer or employee knows or has reason to believe to be an agent or representative of any foreign government , any information of a kind which shall have been classified by the President (or by the head of any such department, agency, or corporation with the approval of the President) as affecting the security of the United States, knowing or having reason to know that such information has been so classified, unless such officer or employee shall have been specifically authorized by the President, or by the head of the department, agency, or corporation by which this officer or employee is employed, to make such disclosure of such information.

[85] 50 U.S.C. 783(b) provides:

> Receipt of, or attempt to receive, by foreign agent or member of Communist organization, classified information. It shall be unlawful for any agent or representative of any foreign government knowingly to obtain or receive, or attempt to obtain or receive, directly or indirectly, from any officer or employee of the United States or of any department or agency thereof or of any corporation the stock of which is owned in whole or in major part by the United States or any department or agency thereof, any information of a kind which shall have been classified by the President (or by the head of any such department, agency, or corporation with the approval of the President) as affecting the security of the United States, unless special authorization for such communication shall first have been obtained from the head of the department, agency, or corporation having custody of or control over such information.

[86] 50 U.S.C. §783(c).

[87] *Id*.

[88] 50 U.S.C. §783(e).

[89] It appears the intent element is satisfied by proof that the material was obtained or disclosed "with intent or reason to believe that the information is to be used [or could be used] to the injury of the United States, or to the advantage of any foreign nation." 18 U.S.C. §§793 and 794. This has been interpreted to require the prosecution to demonstrate a "bad purpose." *See* United States v. Morison, 844 F.2d 1057, 1071 ("An act is done willfully if it is done voluntarily and intentionally and with the specific intent to do something that the law forbids. That is to say, with a bad purpose either to disobey or to disregard the law."). If any of the disclosed material involves communications intelligence as described in 18 U.S.C. §798, the conduct must be undertaken knowingly and willfully to meet the intent threshold.

[90] *See* New York Times Co. v. United States, 403 U.S. 713, 721-22 (1971) (Douglas, J., concurring) (rejecting government argument that term "communicate" should be read to include "publish," based on conspicuous absence of (continued...)

proscribed in 18 U.S.C. Section 794(a), either, although it is possible that publishing covered information in the media could be construed as an "indirect" transmission of such information to a foreign party, as long as the intent that the information reach said party can be demonstrated.[91] The death penalty is available under that subsection if the offense results in the identification and subsequent death of "an individual acting as an agent of the United States,"[92] or the disclosure of information relating to certain other broadly defined defense matters. The word "publishes" does appear in 18 U.S.C. Section 794(b), which applies to wartime disclosures of information related to the "public defense" that "might be useful to the enemy" and is in fact intended to be communicated to the enemy. The types of information covered seem to be limited to military plans and information about fortifications and the like, which may exclude data related to purely historical matters.

Moreover, the statutes described in the previous section have been used almost exclusively to prosecute individuals with access to classified information (and a corresponding obligation to protect it) who make it available to foreign agents, or to foreign agents who obtain classified information unlawfully while present in the United States. Leaks of classified information to the press have only rarely been punished as crimes, and CRS is aware of no case in which a publisher of information obtained through unauthorized disclosure by a government employee has been prosecuted for publishing it. There may be First Amendment implications that would make such a prosecution difficult, not to mention political ramifications based on concerns about government censorship. To the extent that the investigation implicates any foreign nationals whose conduct occurred entirely overseas, any resulting prosecution may carry foreign policy implications related to the exercise of extraterritorial jurisdiction and whether suspected persons may be extradited to the United States under applicable treaty provisions.

Jurisdictional Reach of Relevant Statutes

The Espionage Act gives no express indication that it is intended to apply extraterritorially, but courts have not been reluctant to apply it to overseas conduct of Americans, in particular because Congress in 1961 eliminated a provision restricting the act to apply only "within the admiralty and maritime jurisdiction of the United States and on the high seas, as well as within the United States."[93] This does not answer the question whether the act is intended to apply to foreigners

(...continued)

the term "publish" in that section of the Espionage Act and legislative history demonstrating Congress had rejected an effort to reach publication).

[91] *See* Harold Edgar and Benno C. Schmidt, Jr., *Curtiss-Wright Comes Home: Executive Power and National Security Secrecy*, 21 HARV. C.R.-C.L. L. REV. 349, 395 (1986) (questioning whether Espionage Act can be construed to except publication).

[92] The data released by WikiLeaks contains some names of Afghans who assisted Coalition Forces, leading to some concern that the Taliban might use the information to seek out those individuals for retaliation. *See* Eric Schmitt and David E. Sanger, *Gates Cites Peril in Leak of Afghan War Logs*, N.Y. TIMES, August 2, 2010, at 4. The *New York Times*, *The Guardian*, and *Der Spiegel* published excerpts of the database, but did not publish the names of individual Afghans. *Id*. No deaths have yet been tied to the leaks. *See* Robert Burns, *Pentagon Sees Deadly Risk in Wikileaks Disclosures*, AP NEWSWIRE, August 17, 2010. There appears to be no court precedent interpreting "agent of the United States" in the context of18 U.S.C. §794(a).

[93] *See* United States v. Zehe, 601 F. Supp. 196, 198 (D.C. Mass. 1985)(citing former 18 U.S.C. §791 repealed by P.L. 87-369, 75 Stat. 795(1961)).

outside the United States. Because espionage is recognized as a form of treason,[94] which generally applies only to persons who owe allegiance to the United States, it might be supposed that Congress did not regard it as a crime that could be committed by aliens with no connection to the United States. However, the only court that appears to have addressed the question concluded otherwise.[95] A district court judge held in 1985 that a citizen of East Germany could be prosecuted under Sections 793(b), 794(a) and 794(c) for having (1) unlawfully sought and obtained information regarding the U.S. national defense, (2) delivered that information to his own government, and (3) conspired to do so with the intent that the information be used to the injury of the United States or to the advantage of the German Democratic Republic, all of which offenses were committed within East Germany or in Mexico. The court rejected the defendant's contention that construing the act to cover him would permit the prosecution of noncitizens "who might merely have reviewed defense documents supplied to them by their respective governments."[96] The court considered the scenario unlikely, stating, "Under the statutorily defined crimes of espionage in §§793 and 794, noncitizens would be subject to prosecution only if they actively sought out and obtained or delivered defense information to a foreign government or conspired to do so."[97]

Under this construction, it is possible that noncitizens involved in publishing materials disclosed to them by another would be subject to prosecution only if it can be demonstrated that they took an active role in obtaining the information. The case was not appealed. The defendant, Dr. Alfred Zehe, pleaded guilty in February, 1985 and was sentenced to eight years in prison, but was traded as part of a "spy swap" with East Germany in June of that year.[98]

Application of the Espionage Act to persons who do not hold a position of trust with the government, outside of the classic espionage scenario (in which an agent of a foreign government delivers damaging information to such hostile government), has been controversial. The only known case of that type involved two pro-Israel lobbyists in Washington, Steven J. Rosen and Keith Weissman, associated with the American Israel Public Affairs Committee (AIPAC), who were indicted in 2005 for conspiracy to disclose national security secrets to unauthorized individuals, including Israeli officials, other AIPAC personnel, and a reporter for the *Washington Post*.[99] Their part in the conspiracy amounted to receiving information from government employees with knowledge that the employees were not authorized to disclose it.[100] The

[94] *See* 70 AM. JUR. 2D Sedition, Subversive Activities and Treason §15 (2005). Courts have not been persuaded that the Treason Clause of the Constitution requires the safeguards associated with treason apply also to similar crimes such as espionage or levying war against the United States. *See id.*; United States v. Rosenberg, 195 F.2d 583 (2d. Cir.), *cert. denied*, 344 U.S. 838 (1952)(espionage); United States v. Rodriguez, 803 F.2d 318 (7th Cir.), *cert. denied*, 480 U.S. 908 (1986) (levying war).

[95] *Zehe* at 198 ("Espionage against the United States, because it is a crime that by definition threatens this country's security, can therefore be punished by Congress even if committed by a noncitizen outside the United States.").

[96] *Id*. at 199.

[97] *Id*.

[98] Henry Giniger and Milt Freudenheim, *Free to Spy Another Day?*, NY TIMES, Jun 16, 1985, at A.4.

[99] *See* United States v. Rosen, 445 F. Supp. 2d 602 (E.D. Va. 2006); Jerry Markon, *U.S. Drops Case Against Ex-Lobbyists*, WASH. POST, May 2, 2009, at A1 (stating the case is the first prosecution under the Espionage Act against civilians not employed by the government).

[100] *See* William E. Lee, *Deep Background: Journalists, Sources, and the Perils of Leaking*, 57 AM. U. L. REV. 1453, 1519 (2007) (opining that "the conspiracy charge especially threatens reporter-source transactions where the reporter promises not to disclose the identity of the source").

prosecution was criticized for effectively "criminalizing the exchange of information,"[101] based in part on the government's theory that the defendants were guilty of solicitation of classified information because they inquired into matters they knew their government informant was not permitted to discuss, something that many journalists consider to be an ordinary part of their job.[102] Charges were eventually dropped, reportedly due to a judge's ruling regarding the government's burden of proving the requisite intent and concerns that classified information would have to be disclosed at trial.[103]

Extradition Issues[104]

Assuming that the Espionage Act does apply to foreign nationals for their conduct overseas, there may be several legal obstacles to the extradition of such a suspect to the United States to face charges under the statute, including the possibility that the crime constitutes a political offense for which extradition is unavailable. Extradition to or from the United States is almost exclusively a creature of treaty. The United States has extradition treaties with more than 100 countries, although there are many countries with which it does not.[105] In addition to providing an explicit list of crimes for which extradition may be granted, most modern extradition treaties also identify various classes of offenses and situations for which extradition may or must be denied.

The "political offense" exception has been a common feature of extradition treaties for almost a century and a half, and the exception appears to be contained in every modern U.S. extradition treaty.[106] A political offense may be characterized as a *pure political offense*, or one that is

[101] *Time to Call It Quits*, WASH. POST, March 11, 2009 (editorial urging Attorney General to drop charges).

[102] *See* William E. Lee, *Probing Secrets: The Press and Inchoate Liability for Newsgathering Crimes*, 36 AM. J. CRIM. L. 129, 132-34 (2009). The solicitation theory relied on a 2008 Supreme Court case finding that solicitation of an illegal transaction is not speech deserving of First Amendment protection. United States v. Williams, 553 U.S. 285 (2008). *See id*. at 133 (citing Brief of the United States at 43-44, United States v. Rosen, 557 F.3d 192 (4th Cir. 2008) (No. 08-4358)). *Williams* had to do with solicitation of child pornography, but Justice Scalia posed as a rhetorical question whether Congress could criminalize solicitation of information thought to be covered by the Espionage Act: "Is Congress prohibited from punishing those who attempt to acquire what they believe to be national-security documents, but which are actually fakes? To ask is to answer." *Williams* at 304.

[103] *See* Markon, *supra* footnote 99 (quoting Dana J. Boente, the acting U.S. attorney in Alexandria, VA, where the trial was scheduled to take place). The judge found the scienter requirement of 18 U.S.C. §793 to require that the defendants must have reason to believe the communication of the information at issue "could be used to the injury of the United States or to the advantage of any foreign nation." 445 F. Supp. 2d at 639. Moreover, the judge limited the definition of "information related to the national defense" to information that is "potentially damaging to the United States or ... useful to an enemy of the United States." *Id.* (citing United States v. Morison, 844 F.2d 1057, 1084 (4th Cir. 1988) (Wilkinson, J., concurring)).

[104] This section is contributed by Michael John Garcia, Legislative Attorney.

[105] A current list of countries with which the United States has an extradition treaty is found in CRS Report 98-958, *Extradition To and From the United States: Overview of the Law and Recent Treaties*, by Michael John Garcia and Charles Doyle, at Appendix A.

[106] *See, e.g.*, Australian Extradition Treaty, art. VII(1), entered into force May 8, 1976, 27 U.S.T. 957 ("Extradition shall not be granted … when the offense in respect of which extradition is requested is of a political character, or the person whose extradition is requested proves that the extradition request has been made for the purpose of trying or punishing him for an offense of a political character."); Ecuadorian Extradition Treaty, art. 3, entered into force November 12, 1872, 18 Stat. 199 (similar); Norwegian Extradition Treaty, art. 7, entered into force March 7, 1980, 31 U.S.T. 5619 (similar); United Kingdom Extradition Treaty, art. 4, entered into force April 26, 2007, S. TREATY DOC. 108-23 ("Extradition shall not be granted if the offense for which extradition is requested is a political offense."); Swedish Extradition Treaty, art. 5, entered into force December 3, 1963, 14 U.S.T. 1845 ("Extradition shall not be granted....[i]f the offense is regarded by the requested State as a political offense or as an offense connected with a (continued...)

directed singularly at a sovereign entity and does not have the features an ordinary crime (e.g., there is no violation of the private rights of individuals),[107] or as a *relative political offense*, meaning an "otherwise common crime[] committed in connection with a political act … or common crimes … committed for political motives or in a political context."[108]

The political offense exception may pose a significant obstacle to the extradition of a foreign national to the United States to face charges under the Espionage Act. Espionage, along with treason and sedition, has been recognized as a quintessential example of a purely political offense,[109] although this recognition may arguably apply only to the "classic case" of espionage on behalf of a foreign government by one who owes allegiance to the aggrieved government.[110] Even if the political offense exception applies to the unauthorized disclosure of national defense information, however, the United States could still seek the extradition of a suspect to face other criminal charges (though it would likely be unable to try the fugitive for an offense other than the one for which he was extradited),[111] although extradition might be refused if the charged conduct is deemed to have been committed in furtherance of an act of espionage (or other political offense).[112]

Extradition is also generally limited to crimes identified in the relevant treaty. Early extradition treaties concluded by the United States typically listed specific crimes constituting extraditable offenses.[113] More recent agreements often adopt a dual criminality approach, in which extradition is available when each party recognizes a particular form of misconduct as a punishable offense

(...continued)

political offense.").

[107] Quinn v. Robinson, 783 F.2d 776, 791 (9th Cir. 1986). *See also* M. CHERIF BASSIOUNI, INTERNATIONAL EXTRADITION: UNITED STATES LAW AND PRACTICE (BASSIOUNI) 604 (5th ed. 2007).604; Charles Cantrell, *The Political Offense Exception to Extradition: A Comparison of the United States, Great Britain and the Republic of Ireland*, 60 MARQ. L. REV. 777, 780 (1977).

[108] *Quinn*, 783 F.2d at 791 (internal citations omitted).

[109] *See, e.g., Quinn*, 783 F.2d at 791 (citing treason, sedition, and espionage as examples of purely political offenses); BASSIOUNI, *supra* footnote 107, at 604.

[110] It might be argued that certain offenses punishable under the Espionage Act do not fall under the traditional conception of "espionage," and should therefore not be deemed to be pure political offenses per se. *See generally* PIETRO VERRI, DICTIONARY OF THE INTERNATIONAL LAW OF ARMED CONFLICT 47 (1992) (espionage is "commonly applied to the efforts made in territory under enemy control by a party to the conflict to collect all information on the enemy that may be useful to the conduct of the war in general and to that of hostilities in particular....The word espionage is also applied to the collection by States, in peacetime as well as in time of war, of political and military information regarding each other."); Lt. Col. Geoffrey B. Demarest, *Espionage in International Law*, 24 DENV. J. INT'L L. & POL'Y 321, 324 (1996) ("Throughout history, the terms 'espionage' and 'spying' have carried varying amounts of pejorative baggage. Therefore, any attempt at a precise definition is difficult."). Nonetheless, such an offense might still be deemed to be sufficiently related to political action or informed by political motivations so as to fall under the political offense exception.

[111] Under the doctrine of specialty, sometimes called specialty, "a person who has been brought within the jurisdiction of the court by virtue of proceedings under an extradition treaty, can only be tried for one of the offences described in that treaty, and for the offence with which he is charged in the proceedings for his extradition, until a reasonable time and opportunity have been given him after his release or trial upon such charge, to return to the country from whose asylum he had been forcibly taken under those proceedings." United States v. Alvarez-Machain, 504 U.S. 655, 661 (1992) (*quoting* United States v. Rauscher, 119 U.S. 407, 430 (1886)). This limitation is expressly included in many treaties.

[112] 18 U.S.C. §641

[113] *E.g.*, Ecuadorian Extradition Treaty, art. 2, entered into force November 12, 1872, 18 Stat. 199, as modified by supplementary agreement, entered into force May 29, 1941, 55 Stat. 1196 (authorizing extradition for specific offenses).

(subject to other limitations found elsewhere in the applicable extradition treaty).[114] No U.S. extradition treaty currently in force lists espionage as an extraditable offense.[115] Assuming for the sake of argument that certain espionage offenses are not *per se* political offenses for which extradition may not be granted, it would appear that the United States could only seek the extradition of a foreign national for an espionage offense if the applicable treaty authorized extradition in cases of dual criminality, and the requested state recognized espionage (or perhaps unauthorized receipt or disclosure of protected government information) as a criminal offense under its domestic laws.

Whether extradition is available for an offense occurring outside the United States may depend in part upon whether the applicable treaty covers extraterritorial offenses. As a general rule, crimes are defined by the laws of the place where they are committed.[116] Nations have always been understood to have authority to outlaw and punish conduct occurring outside the confines of their own territory under some circumstances, but the United States now claims more sweeping extraterritorial application for some of its criminal laws than is recognized either in its more historic treaties or by many of today's governments.[117] This may complicate any extradition efforts because many U.S. extradition treaties apply only to crimes "committed within the [territorial] jurisdiction" of the country seeking extradition.[118] Some contemporary treaties call for extradition regardless of where the offense was committed, while perhaps an equal number permit or require denial of an extradition request that falls within an area where the countries hold conflicting views on extraterritorial jurisdiction.[119]

The extradition of a foreign national to the United States to face criminal charges may be impeded by nationality provisions contained in extradition treaties with many countries, which recognize the right of a requested party to refuse to extradite its own nationals. U.S. extradition agreements generally are either silent with respect to nationality, in which case all persons are subject to extradition without regard to their nationality, or they contain a nationality clause that specifies that parties are not bound to deliver up their own nationals, in some cases leaving room

---

[114] *E.g.*, Extradition Agreement with the European Union, art. 4(1), entered into force February 1, 2010, S. TREATY DOC. 109-14 (applying in place of any provision in an earlier extradition agreement between the United States and an EU Member State which only authorized extradition only an exclusive list of offenses, and instead providing that "An offense shall be an extraditable offense if it is punishable under the laws of the requesting and requested States by deprivation of liberty for a maximum period of more than one year or by a more severe penalty"); Protocol to Australian Extradition Treaty, art. 1, entered into force December 21, 1992, S. TREATY DOC. 102-23 (replacing provision of earlier extradition agreement listing specific offenses where extradition was available with a provision requiring dual criminality).

[115] It should be noted, however, that extradition treaties may cover certain offenses that can constitute elements of the crime of espionage (e.g., knowingly receiving or fraudulently obtaining property). *See, e.g.,* Extradition Treaty with Belize, appendix listing extraditable offenses, entered into force March 27, 2001, S. TREATY DOC. 106-38,

[116] *See* CRS Report 94-166, *Extraterritorial Application of American Criminal Law*, by Charles Doyle.

[117] *See* CRS Report 98-958, *Extradition To and From the United States: Overview of the Law and Recent Treaties*, by Michael John Garcia and Charles Doyle. Even among countries holding fairly expansive views of the extraterritorial jurisdiction, there may be substantial differences between the perceptions of common law countries and those of civil law countries, Charles L. Blakesley, *A Conceptual Framework for Extradition and Jurisdiction Over Extraterritorial Crimes*, 1984 UTAH L. REV. 685 (1984).

[118] IV Michael Abbell & Bruno A. Ristau, International Judicial Assistance: Criminal 64-7 (1990). *See, e.g.,* Ecuadorian Extradition Treaty, art. 1, entered into force November 12, 1872, 18 Stat. 199 (applying to offenses "committed within the jurisdiction of one of the contracting parties").

[119] For examples of specific treaties, see CRS Report 98-958, *Extradition To and From the United States: Overview of the Law and Recent Treaties*.

for executive discretion.[120] Some newer treaties declare that "extradition shall not be refused based on the nationality of the person sought," while others limit the nationality exemption to nonviolent crimes or bar nationality from serving as the basis to deny extradition when the fugitive is sought in connection with a listed offense.

The ability of the United States to obtain the extradition of a fugitive for a criminal offense may also be impacted by the existence of competing extradition requests made by other States. The criteria used by a requested State to determine the precedence given to competing extradition requests may be established either by its domestic laws or via its extradition treaties with the requesting countries.[121] If the requested State opts to give priority to the extradition request of another country, it might still be possible for the United States to obtain the extradition of the fugitive at a later date. Whether a fugitive extradited to one State can thereafter be extradited to a third country may depend upon the applicable treaties between the relevant States. Some extradition agreements authorize the requesting State to re-extradite a person to a third country in certain circumstances. Generally, re-extradition is only permitted when the State from whom extradition was initially obtained consents to the re-extradition of the fugitive, or the fugitive voluntarily remains in the State where he was initially extradited for a specified period after having been released from custody.[122]

Constitutional Issues

The publication of information pertaining to the national defense or foreign policy may serve the public interest by providing citizens with information necessary to shed light on the workings of government, but it seems widely accepted that the public release of at least some of such information poses a significant enough threat to the security of the nation that the public interest is better served by keeping it secret. The Constitution protects the public right to access government information and to express opinions regarding the functioning of the government, among other things, but it also charges the government with "providing for the common defense." Policymakers are faced with the task of balancing these interests.

The First Amendment to the U.S. Constitution provides: "Congress shall make no law ... abridging the freedom of speech, or of the press...."[123] Despite this absolute language, the

[120] BASSIOUNI, *supra* footnote 107, at 739.

[121] Extradition Agreement with the European Union, art. 10, entered into force February 1, 2010, S. TREATY DOC. 109-14 (describing factors to be considered by requested State when considering competing extradition requests from the United States or other EU Member States); Bolivian Extradition Treaty, art. X, entered into force November 21, 1996, S. TREATY DOC. 104-22.

[122] *See, e.g.,* Swedish Extradition Treaty, art. IX, entered into force December 3, 1963, 14 U.S.T. 1845 ("A person extradited by virtue of this Convention may not be tried or punished by the requesting State for any offense committed prior to his extradition, other than that which gave rise to the request, nor may he be re-extradited by the requesting State to a third country which claims him, unless the surrendering State so agrees or unless the person extradited, having been set at liberty within the requesting State, remains voluntarily in the requesting State for more than 45 days from the date on which he was released. Upon such release, he shall be informed of the consequences to which his stay in the territory of the requesting State might subject him."); Turkish Extradition Treaty, art. 17, entered into force January 1, 1987, 32 UST 2111 (similar). *See also* Council of Europe, Convention on Extradition, art. 15, done December 13, 1957 (providing similar requirements for re-extradition among member States of the Council of Europe), *available at* http://conventions.coe.int/Treaty/EN/Treaties/Html/024.htm.

[123] For an analysis of exceptions to the First Amendment, see CRS Report 95-815, *Freedom of Speech and Press: Exceptions to the First Amendment*, by Kathleen Ann Ruane.

Supreme Court has held that "[t]he Government may ... regulate the content of constitutionally protected speech in order to promote a compelling interest if it chooses the least restrictive means to further the articulated interest."[124]

Where speech is restricted based on its content, the Supreme Court generally applies "strict scrutiny," which means that it will uphold a content-based restriction only if it is necessary "to promote a compelling interest," and is "the least restrictive means to further the articulated interest."[125] Protection of the national security from external threat is without doubt a compelling government interest.[126] It has long been accepted that the government has a compelling need to suppress certain types of speech, particularly during time of war or heightened risk of hostilities.[127] Speech likely to incite immediate violence, for example, may be suppressed.[128] Speech that would give military advantage to a foreign enemy is also susceptible to government regulation.[129]

Where First Amendment rights are implicated, it is the government's burden to show that its interest is sufficiently compelling to justify enforcement. Whether the government has a compelling need to punish disclosures of classified information turns on whether the disclosure has the potential of causing damage to the national defense or foreign relations of the United States.[130] Actual damage need not be proved, but potential damage must be more than merely speculative and incidental.[131] On the other hand, the Court has stated that "state action to punish the publication of truthful information seldom can satisfy constitutional standards."[132] And it has described the constitutional purpose behind the guarantee of press freedom as the protection of "the free discussion of governmental affairs."[133]

---

[124] Sable Communications of California v. Federal Communications Commission, 492 U.S. 115, 126 (1989).

[125] *Id.*

[126] *See* Haig v. Agee, 453 U.S. 280 (1981) ("It is 'obvious and unarguable' that no governmental interest is more compelling than the security of the Nation.")(citing Aptheker v. Secretary of State, 378 U.S. 500, 509; *accord* Cole v. Young, 351 U.S. 536, 546 (1956)).

[127] See Schenck v. United States, 249 U.S. 47 (1919) (formulating "clear and present danger" test).

[128] Brandenburg v. Ohio, 395 U.S. 444 (1969).

[129] Near v. Minnesota, 283 U.S. 697, 716 (1931) ("No one would question but that a government might prevent actual obstruction to its recruiting service or the publication of the sailing dates of transports or the number and location of troops.").

[130] "National Security" is defined as national defense and foreign relations. *See* Exec. Order No. 13526, 75 Fed. Reg. 707 §6.1(cc) (January 5, 2010).

[131] *See, e.g.,* New York Times Co. v. United States, 403 U.S. 713, 725 (1971) (Brennan, J., concurring) (rejecting as insufficient government's assertions that publication of Pentagon Papers "could," "might," or "may" prejudice the national interest); Elrod v. Burns, 427 U.S. 347, 362 (1976) ("The interest advanced must be paramount, one of vital importance, and the burden is on the government to show the existence of such an interest.") (citing Buckley v. Valeo, 424 U.S. 1, 94(1976); Williams v. Rhodes, 393 U.S. 23, 31-33(1968); NAACP v. Button, 371 U.S. 38, 45 (1963); Bates v. Little Rock, 361 U.S. 516, 524 (1960); NAACP v. Alabama, 357 U.S. 449, 464-466 (1958); Thomas v. Collins, 323 U.S. 516, 530 (1945)).

[132] Bartnicki v. Vopper, 532 U.S. 514, 527 (2001) (citing Smith v. Daily Mail Publishing Co., 443 U.S. 97 (1979)).

[133] Mills v. Alabama, 384 U.S. 214, 218 (1966). Because of the First Amendment purpose to protect the public's ability to discuss governmental affairs along with court decisions denying that it provides any special rights to journalists, *e.g.*, Branzburg v. Hayes, 408 U.S. 665 (1972), it is not likely a plausible argument to posit that it does not apply to the *foreign* press. *See* United States v. 18 Packages of Magazines 238 F. Supp. 846, 847-848 (D.C. Cal. 1964) ("Even if it be conceded, arguendo, that the 'foreign press' is not a direct beneficiary of the Amendment, the concession gains nought for the Government in this case. The First Amendment does protect the public of this country. … The First Amendment surely was designed to protect the rights of readers and distributors of publications no less than those of (continued...)

Although information properly classified in accordance with statute or executive order carries by definition, if disclosed to a person not authorized to receive it, the potential of causing at least identifiable harm to the national security of the United States,[134] it does not necessarily follow that government classification by itself will be dispositive of the issue in the context of a criminal trial. However, courts have adopted as an element of the espionage statutes a requirement that the information at issue must be "closely held."[135] Government classification will likely serve as strong evidence to support that contention, even if the information seems relatively innocuous or does not contain much that is not already publicly known.[136] Typically, courts have been unwilling to review decisions of the executive related to national security, or have made a strong presumption that the material at issue is potentially damaging.[137] Still, judges have recognized that the government must make *some* showing that the release of specific national defense information has the potential of harming U.S. interests, lest the Espionage Act become a means to punish whistle-blowers who reveal information that poses more of a danger of embarrassing public officials than of endangering national security.[138]

(...continued)

writers or printers. Indeed, the essence of the First Amendment right to freedom of the press is not so much the right to print as it is the right to read. The rights of readers are not to be curtailed because of the geographical origin of printed materials."). The Supreme Court invalidated, on First Amendment grounds, a statute that required postal authorities to detain unsealed mail from abroad deemed to contain "communist political propaganda" unless the recipient affirms a desire to receive it. Lamont v. Postmaster General, 381 U.S. 301 (1965).

Likewise, the fact that WikiLeaks is not a typical newsgathering and publishing organization would likely make little difference under First Amendment analysis. The Supreme Court has not established clear boundaries between the protection of speech and that of the press, nor has it sought to develop criteria for identifying what constitutes "the press" that might qualify its members for privileges not available to anyone else. *See generally* CONGRESSIONAL RESEARCH SERVICE, THE CONSTITUTION OF THE UNITED STATES: ANALYSIS AND INTERPRETATION, SEN. DOC. NO. 108-17, at 1083-86 (2002), *available at* http://crs.gov/conan/default.aspx?mode=topic&doc=Amendment01.xml&t=2|3.

[134] Exec. Order No. 13526, 75 Fed. Reg. 707 §1.2 (January 5, 2010) ("Classified National Security Information").

Section 1.3 defines three levels of classification:

> (1) "Top Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause *exceptionally grave damage* to the national security that the original classification authority is able to identify or describe.
>
> (2) "Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause *serious damage* to the national security that the original classification authority is able to identify or describe.
>
> (3) "Confidential" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause *damage* to the national security that the original classification authority is able to identify or describe.

[135] United States v. Heine, 151 F.2d 813 (2d Cir.1945) (information must be "closely held" to be considered "related to the national defense" within the meaning of the espionage statutes).

[136] *See*, *e.g.,* United States v. Abu-Jihaad 600 F.Supp.2d 362, 385 -386 (D. Conn. 2009) (although completely inaccurate information might not be covered, information related to the scheduled movements of naval vessels was sufficient to bring materials within the ambit of national defense information).

[137] *See, e.g.,* Haig v. Agee, 453 U.S. 280, 291 (1981) ("Matters intimately related to foreign policy and national security are rarely proper subjects for judicial intervention.").

[138] *See*, *e.g.*, United States v. Morison, 844 F.2d 1057, 1086 (4th Cir. 1988) (Phillips, J., concurring) ("… I assume we reaffirm today, that notwithstanding information may have been classified, the government must still be required to prove that it was *in fact* 'potentially damaging ... or useful,' i.e., that the fact of classification is merely probative, not conclusive, on that issue, though it must be conclusive on the question of authority to possess or receive the information. This must be so to avoid converting the Espionage Act into the simple Government Secrets Act which Congress has refused to enact.") (emphasis in original).

The Supreme Court seems satisfied that national security is a vital interest sufficient to justify some intrusion into activities that would otherwise be protected by the First Amendment—at least with respect to federal employees. Although the Court has not held that government classification of material is sufficient to show that its release is damaging to the national security,[139] it has seemed to accept without much discussion the government's assertion that the material in question is damaging. It is unlikely that a defendant's bare assertion that information poses no danger to U.S. national security will be persuasive without some convincing evidence to that effect, or proof that the information is not closely guarded by the government.[140]

A challenge to the Espionage Act has reached the Supreme Court for decision in only one instance. In *Gorin v. United States*,[141] the Court upheld portions of the act now codified as 18 U.S.C. Sections 793 and 794 against assertions of vagueness, but only because jury instructions properly established the elements of the crimes, including the scienter requirement (proof of "guilty knowledge") and a definition of "national defense" that includes potential damage in case of unauthorized release of protected information and materials. *Gorin* was a "classic case" of espionage, and did not involve a challenge based on the First Amendment right to free speech. The Court agreed with the government that the term "national defense" was not vague; it was satisfied that the term describes "a generic concept of broad connotations, referring to the military and naval establishments and the related activities of national preparedness."[142] Whether information was "related to the national defense" was a question for the jury to decide,[143] based on its determination that the information "may relate or pertain to the usefulness, efficiency or availability of any of the above places, instrumentalities or things for the defense of the United States of America. The connection must not be a strained one nor an arbitrary one. The relationship must be reasonable and direct."[144] As long as the jury was properly instructed that only information likely to cause damage meets the definition of information "related to the national defense" for the purpose of the statute, the term was not unconstitutionally vague.

United States v. Morison[145] is significant in that it represents the first case in which a person was convicted for selling classified documents to the media.[146] Samuel Loring Morison, charged with providing classified satellite photographs to the British defense periodical *Jane's Defence Weekly*, argued that the espionage statutes did not apply to his conduct because he could not have had the requisite intent to commit espionage. The Fourth Circuit rejected his appeal, finding the intent to sell photographs that he clearly knew to be classified sufficient to satisfy the scienter requirement under 18 U.S.C. Section 793(d) (disclosure by lawful possessor of defense information to one not

[139] *See, e.g.*, Scarbeck v. United States, 317 F.2d 546 (D.C. Cir. 1962) (holding government did not have to show documents were *properly* classified "as affecting the national defense" to convict employee under 50 U.S.C. §783, which prohibits government employees from transmitting classified documents to foreign agents or entities).

[140] *See* United States v. Dedeyan, 594 F.2d 36, 39 (4th Cir. 1978).

[141] 312 U.S. 19 (1941).

[142] *Id.* at 28.

[143] *Id.* at 32. The information defendant was charged with passing to the Soviet government had to do with U.S. intelligence on the activities of Japanese citizens in the United States.

[144] *Id.* at 31.

[145] 844 F.2d 1057 (4th Cir.), *cert. denied,* 488 U.S. 908 (1988).

[146] Efforts to prosecute Daniel Ellsberg and Anthony Russo in connection with the disclosure of the Pentagon Papers were unsuccessful after the judge dismissed them for prosecutorial misconduct. More recently, a Defense Department employee pleaded guilty to charges under the Espionage Act for disclosing classified material to lobbyists and to journalists. United States v. Franklin, Cr. No. 05-225 (E.D. Va., 2005). For a description of these and other relevant cases, see Lee, *supra* footnote 100.

entitled to receive it). The definition of "relating to the national defense" was held not to be overbroad because the jury had been instructed that the government had the burden of showing that the information was so related.[147] His assertedly laudable motive in permitting publication of the photographs was not found to negate the element of intent.[148]

The fact that the Morison prosecution involved a leak to the media with no obvious intent to transmit sensitive information to hostile intelligence services did not persuade the jury or the judges involved that he lacked culpability, but the Justice Department did come under some criticism on the basis that such prosecutions are so rare as to amount to a selective prosecution in his case, and that it raised concerns about the chilling effect such prosecutions could have on would-be whistle-blowers who could provide information embarrassing to the government but vital to public discourse.[149] On leaving office, President Clinton pardoned Morison.[150]

As far as the possible prosecution of the publisher of information leaked by a government employee is concerned, the most relevant case is likely to be the *Pentagon Papers* case.[151] To be sure, the case involved an injunction against publication rather than a prosecution for having published information, but the rationale for protecting such disclosure may nevertheless inform any decision involving a conviction. In a *per curiam* opinion accompanied by nine concurring or dissenting opinions, the U.S. Supreme Court refused to grant the government's request for an injunction to prevent the *New York Times* and the *Washington Post* from printing a classified study of the U.S. involvement in Vietnam. The Court explained:

> prior restraints are the most serious and least tolerable infringement on First Amendment rights.... A prior restraint, ... by definition, has an immediate and irreversible sanction. If it can be said that a threat of criminal or civil sanctions after publication "chills" speech, prior restraint "freezes" it at least for the time. The damage can be particularly great when the prior restraint falls upon the communication of news and commentary on current events.[152]

A majority of the justices suggested in separate *dicta* that the newspapers—along with the former government employee who leaked the documents to the press—could be prosecuted under the Espionage Act.[153] Still, in later cases the Court stressed that any prosecution of a publisher for

---

[147] *But see* Scarbeck v. United States, 317 F.2d 546 (D.C. Cir. 1962) (holding that government did not need to prove proper classification of documents to prove a violation).

[148] 844 F.2d at 1073-74. Morison had stated that he sought the publication of the photos because they would demonstrate to the public the gravity of the threat posed by the Soviet Union, which he hoped would result in an increased defense budget. *See* P. Weiss, *The Quiet Coup: U.S. v. Morison - A Victory for Secret Government*, HARPER'S, September 1989.

[149] *See* Jack Nelson, *U.S. Government Secrecy and the Current Crackdown on Leaks* 8, The Joan Shorenstein Center on the Press, Politics and Public Policy, Working Paper Series 2003-1 (2002), *available at* http://www.hks.harvard.edu/presspol/publications/papers/working_papers/2003_01_nelson.pdf.

[150] Valerie Strauss, *Navy Analyst Morison Receives a Pardon*, WASH. POST, January 21, 2001, at A17. Senator Daniel Patrick Moynihan wrote a letter in support of Morison's pardon and explaining his view that "An evenhanded prosecution of leakers could imperil an entire administration," and that "[i]f ever there were to be widespread action taken, it would significantly hamper the ability of the press to function." Letter, Sen. Daniel Patrick Moynihan to President Clinton, September 29, 1998, *available at* http://www.fas.org/sgp/news/2001/04/moynihan.html.

[151] New York Times Co. v. United States, 403 U.S. 713 (1971) (per curiam).

[152] Nebraska Press Association v. Stuart, 427 U.S. 539, 559 (1976) (striking down a court order restraining the publication or broadcast of accounts of confessions or admissions made by the defendant at a criminal trial).

[153] 403 U.S. at 734-40 (White, J. with Stewart, J. concurring); *id*. at 745-47 (Marshall, J., concurring); *id*. at 752 (Burger, C.J., dissenting); *id*. at 752-59 (Harlan, J., joined by Burger, C.J. and Blackmun, J., dissenting). *See* David Topol, Note, *United States v. Morison: A Threat to the First Amendment Right to Publish Security Information*, 43 S.C. (continued...)

what has already been printed would have to overcome only slightly less insurmountable hurdles.[154] Moreover, if national security interests were not sufficient to outweigh the First Amendment principles implicated in the prior restraint of pure speech related to the public interest, as in the *Pentagon Papers* case,[155] it is difficult to discern an obvious rationale for finding that punishing that same speech after it has already been disseminated nevertheless tilts the balance in favor of the government's interest in protecting sensitive information.

The publication of truthful information that is lawfully acquired enjoys considerable First Amendment protection.[156] The Court has not resolved the question "whether, in cases where information has been acquired *unlawfully* by a newspaper or by a source, government may ever punish not only the unlawful acquisition, but the ensuing publication as well."[157] (The *Pentagon Papers* Court did not consider whether the newspapers' receipt of the classified document was in itself unlawful, although it appeared to accept that the documents had been unlawfully taken from the government by their source.)

The Court has established that "routine newsgathering" is presumptively lawful acquisition, the fruits of which may be published without fear of government retribution.[158] However, what constitutes "routine newsgathering" has not been further elucidated. In the 2001 case *Bartnicki v. Vopper*, the Court cited the *Pentagon Papers* case to hold that media organizations cannot be punished (albeit in the context of civil damages) for divulging information on the basis that it had been obtained unlawfully by a third party.[159] The holding suggests that recipients of unlawfully disclosed information cannot be considered to have obtained such material unlawfully based solely on their knowledge (or "reason to know") that the discloser acted unlawfully. Under such circumstances, disclosure of the information by the innocent recipient would be covered by the First Amendment, although a wrongful disclosure by a person in violation of an obligation of trust would receive no First Amendment protection, regardless of whether the information was obtained lawfully.[160]

Bartnicki had to do with the disclosure of illegally intercepted communications in violation of federal and state wiretap laws, which prohibited disclosure of such information by anyone who

(...continued)

L. REV. 581, 586 (noting that three concurring justices suggested that the government could convict the newspapers under the Espionage Act even though it could not enjoin them from printing the documents, while the three dissenting justices thought the injunction should issue).

[154] Smith v. Daily Mail Publishing Co., 443 U.S. 97, 102-03 (1979) ("Whether we view the statute as a prior restraint or as a penal sanction for publishing lawfully obtained, truthful information is not dispositive because even the latter action requires the highest form of state interest to sustain its validity.") The case involved the prosecution of a newspaper for publishing the name of a juvenile defendant without court permission, in violation of state law.

[155] For a list of the types of damage the government argued would ensue if its efforts to enjoin publication failed, see William H. Freivogel, *Publishing National Security Secrets: The Case for "Benign Indeterminacy,"* 3 J. NAT'L SECURITY L. & POL'Y 95, 112-13 (2009).

[156] *See*, *e.g.*, Landmark Commc'ns. v. Virginia, 435 U.S. 829, 837 (1978).

[157] Florida Star v. B.J.F. 491 U.S. 524, 535 (1989). The Court also questioned whether the receipt of information can ever constitutionally be proscribed. *Id.* at 536.

[158] *Daily Mail*, 443 U.S at 103. Here, routine newsgathering consisted of perusing publicly available court records.

[159] 532 U.S. 514 (2001).

[160] *See* Boehner v. McDermott, 484 F.3d 573 (D.C. Cir. 2007) (en banc) (Congressman, bound by Ethics Committee rules not to disclose certain information, had no First Amendment right to disclose to press contents of tape recording illegally made by third party).

knew or had reason to know that it was the product of an unlawful interception, but did not prohibit the *receipt* of such information. The Espionage Act, by contrast, does expressly prohibit the receipt of certain national defense material with knowledge or reason to believe that it "has been or will be obtained, taken, made, or disposed of" contrary to the provisions of the act.[161] This distinction could possibly affect whether a court would view the information as having been lawfully acquired; although the *Bartnicki* opinion seems to establish that knowledge that the information was unlawfully disclosed by the initial leaker cannot by itself make receipt or subsequent publication unlawful, it does not directly address whether knowledge of the nature of the information received would bring about a different result.

Prior Legislative Efforts

The current laws protecting classified information have been criticized as a patchwork of mostly outdated provisions that are vague and inconsistent, or that they may not cover all the information the government legitimately needs to protect.[162] Conversely, others argue that they fail to take due consideration of the value of releasing to the public information that the government would prefer to keep out of view.[163]

The Classified Information Protection Act of 2001

In 2000, and again in 2001-2002, Congress sought to create 18 U.S.C. Section 798A, subsection (a) of which would have read:

> Whoever, being an officer or employee of the United States, a former or retired officer or employee of the United States, any other person with authorized access to classified information, or any other person formerly with authorized access to classified information, knowingly and willfully discloses, or attempts to disclose, any classified information acquired as a result of such person's authorized access to classified information to a person (other than an officer or employee of the United States) who is not authorized access to such classified information, knowing that the person is not authorized access to such classified information, shall be fined under this title, imprisoned not more than 3 years, or both.[164]

The proposed provision would have penalized the disclosure of any material designated as classified for any reason related to national security, regardless of whether the violator intended that the information be delivered to and used by foreign agents (in contrast to 50 U.S.C. Section 783). It would have been the first law to penalize disclosure of information to entities other than foreign governments or their equivalent solely because it is classified, without a more specific definition of the type of information covered.[165] In short, the provision would have made it a

[161] 18 U.S.C. §793(c). The provision does not appear to cover receipt of intangible information.

[162] *See*, *e.g.*, The Espionage Act and the Legal and Constitutional Issues Raised by WikiLeaks, Hearing before the H. Comm. on the Judiciary, 111th Cong. (2010).

[163] *See id*.

[164] H.R. 4392, 106th Cong. §304 (enrolled bill); H.R. 2943, 107th Cong; Previous unsuccessful bills to criminalize leaks of classified information by government officers and employees include H.R. 319, 104th Cong. (providing for prison term up to 20 years as well as possible fine); H.R. 271, 103d Cong. (same); H.R. 363, 102d Cong. (same); H.R. 279, 101st Cong.; H.R. 3066, 100th Cong.; H.R. 3468, 96th Cong (would have excluded non-government employees from accomplice liability); H.R. 6057, 95th Cong.; H.R. 13602, 94th Cong.

[165] 18 USCS §1924 prohibits removal of government-owned or controlled classified information by a government (continued...)

crime to disclose or attempt to disclose classified information[166] to any person who does not have authorized access to such information, with exceptions covering disclosures to Article III courts, or to the Senate or House committees or members, and for authorized disclosures to persons acting on behalf of a foreign power (including an international organization). The provision would have amended the espionage laws in title 18 by expanding the scope of information they cover. The proposed language was intended to make it easier for the government to prosecute unauthorized disclosures of classified information, or "leaks" of information that might not amount to a violation of current statutes. The language was intended to ease the government's burden of proof in such cases by eliminating the need "to prove that damage to the national security has or will result from the unauthorized disclosure,"[167] substituting a requirement to show that the unauthorized disclosure was of information that "is or has been properly classified" under a statute or executive order.

The 106th Congress passed the measure as part of the Intelligence Authorization Act for Fiscal Year 2001,[168] but President Clinton vetoed it, calling it "well-intentioned" as an effort to deal with legitimate concerns about the damage caused by unauthorized disclosures, but "badly flawed" in that it was "overbroad" and posed a risk of "unnecessarily chill[ing] legitimate activities that are at the heart of a democracy."[169] President Clinton explained his view that

> [a] desire to avoid the risk that their good faith choice of words—their exercise of judgment—could become the subject of a criminal referral for prosecution might discourage Government officials from engaging even in appropriate public discussion, press briefings, or other legitimate official activities. Similarly, the legislation may unduly restrain the ability of former Government officials to teach, write, or engage in any activity aimed at building public understanding of complex issues. Incurring such risks is unnecessary and inappropriate in a society built on freedom of expression and the consent of the governed and is particularly inadvisable in a context in which the range of classified materials is so extensive. In such circumstances, this criminal provision would, in my view, create an undue chilling effect.[170]

The 107th Congress considered passing an identical provision,[171] but instead directed the Attorney General and heads of other departments to undertake a review of the current protections against the unauthorized disclosure of classified information, and to issue a report recommending

(...continued)

employee without authorization. 50 U.S.C. §783 covers only information classified by the President or an executive agency transmitted by a government employee to a foreign government. 18 U.S.C. §§793 and 794 are potentially broader than these in that they cover information "related to the national defense," by government employees and others without regard to the identity of the recipient of the information, but these require intent or knowledge regarding harm to the national defense.

[166] "Classified information" was defined in the proposed measure to mean "information or material designated and clearly marked or represented, or that the person knows or has reason to believe has been determined by appropriate authorities, pursuant to the provisions of a statute or Executive Order, as requiring protection against unauthorized disclosure for reasons of national security."

[167] *See* H.Rept. 106-969 at 44 (2000).

[168] H.R. 4392 §304, 106th Congress.

[169] Message on Returning Without Approval to the House of Representatives the "Intelligence Authorization Act for Fiscal Year 2001", 36 WEEKLY COMP. PRES. DOC. 278 (November 4, 2000).

[170] *Id*.

[171] The Classified Information Protection Act of 2001, H.R. 2943, 107th Cong;

legislative or administrative actions.[172] An identical measure was introduced late in the 109th Congress, but was not reported out of committee.[173]

The Attorney General, in his report to the 108th Congress, concluded that

> [a]lthough there is no single statute that provides criminal penalties for all types of unauthorized disclosures of classified information, unauthorized disclosures of classified information fall within the scope of various current statutory criminal prohibitions. It must be acknowledged that there is no comprehensive statute that provides criminal penalties for the unauthorized disclosure of classified information irrespective of the type of information or recipient involved. Given the nature of unauthorized disclosures of classified information that have occurred, however, I conclude that current statutes provide a legal basis to prosecute those who engage in unauthorized disclosures, if they can be identified. It may be that carefully drafted legislation specifically tailored to unauthorized disclosures of classified information generally, rather than to espionage, could enhance our investigative efforts. The extent to which such a provision would yield any practical additional benefits to the government in terms of improving our ability to identify those who engage in unauthorized disclosures of classified information or deterring such activity is unclear, however.[174]

Current Proposals

The Securing Human Intelligence and Enforcing Lawful Dissemination Act ("SHIELD Act"), S. 315,[175] introduced by Senator Ensign on February 10, 2011, and a companion bill in the House, H.R. 703,[176] would amend 18 U.S.C. Section 798 to add coverage for disclosures of classified information related to human intelligence activities (the provision currently covers only certain information related to communications intelligence). The bills would add "transnational threat" to the entities whose benefit from unlawful disclosures would make such disclosure illegal. The statute as written prohibits disclosure of classified information for the benefit of any foreign government (or to the detriment of the United States, which would remain unchanged if the bill is enacted). A "transnational threat" for purposes of the bills means any ''any 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 any person or group who engages in any of these activities. This change is likely intended to ensure that disclosures of any covered information that a violator "publishes, or uses in any manner … for the benefit" of Al Qaeda or any other terrorist group, international drug cartels, arms dealers who traffic in weapons of mass destruction, and other international criminals will be subject to prosecution, regardless of whether the group purports to govern any territory. As is currently the case, it is unclear whether this conduct must be undertaken "knowingly and willfully" to incur a punishment, or whether those qualifiers apply only to furnishing covered information to an unauthorized individual.

The bills would add two types of information to be covered by the prohibition: "information concerning the human intelligence activities of the United States or any foreign government"; and

[172] Intelligence Authorization Act for Fiscal Year 2002, P.L. 107-108, §310 (2001).

[173] S. 3774, 109th Cong.

[174] Report to Congress on Unauthorized Disclosure of Classified Information, October 15, 2002 (citations omitted).

[175] The bill was introduced at the end of the 111th Congress as S. 4004.

[176] A substantially identical bill was introduced as H.R. 6506 at the end of the 111th Congress.

"information concerning the identity of a classified source or informant of an element of the intelligence community of the United States." "Human intelligence" is defined under the bills as "all procedures, sources, and methods employed in the collection of intelligence through human sources." "Classified information" would be defined, as in the current provision, as "information which, at the time of a violation of this section, is, for reasons of national security, specifically designated by a United States Government Agency for limited or restricted dissemination or distribution." In other words, the information need not be classified information within the meaning of the executive order, so long as it has been specifically designated as subject to some form of restricted dissemination due to national security concerns. Because the concept of national security includes foreign affairs as well as national defense, the information covered may already be broader than that protected under the preceding sections of the Espionage Act. However, the proposed limitation on the identity of informants and sources to those giving information to an element of the intelligence community may be interpreted to exclude informants and sources who provide information to entities not listed in 50 U.S.C. Section 401a(4), such as infantry units or consular offices.[177]

Senator Cardin introduced the Espionage Statutes Modernization Act of 2010, S. 355, on February 15, 2011.[178] This bill would broaden the Espionage Act provisions by extending their coverage to all classified information related to the national security (rather than merely national defense information) and would incorporate non-state threats into the prohibition by substituting "foreign power" (as defined under the Foreign Intelligence Surveillance Act, at 50 U.S.C. Section 1801) for "foreign government" or "foreign nation." The bill also includes a new provision to be codified at 18 U.S.C. Section 1925 to prohibit the intentional unauthorized disclosure of properly classified information by government employees, contractors, or consultants in violation of the terms of a nondisclosure agreement, provides for extraterritorial jurisdiction over the offense, and instructs the U.S. Sentencing Commission to review and amend as appropriate the Sentencing

[177] Only the House bill defines "Intelligence Community" with reference to 50 U.S.C. §401a(4), H.R. 703 §2(b), but the definition could be inferred for purposes of the Senate bill, which does not define "intelligence community." 50 U.S.C. §401(a)(4) defines intelligence community to include

> (A) The Office of the Director of National Intelligence.
>
> (B) The Central Intelligence Agency.
>
> (C) The National Security Agency.
>
> (D) The Defense Intelligence Agency.
>
> (E) The National Geospatial-Intelligence Agency.
>
> (F) The National Reconnaissance Office.
>
> (G) Other offices within the Department of Defense for the collection of specialized national intelligence through reconnaissance programs.
>
> (H) The intelligence elements of the Army, the Navy, the Air Force, the Marine Corps, the Federal Bureau of Investigation, and the Department of Energy.
>
> (I) The Bureau of Intelligence and Research of the Department of State.
>
> (J) The Office of Intelligence and Analysis of the Department of the Treasury.
>
> (K) The elements of the Department of Homeland Security concerned with the analysis of intelligence information, including the Office of Intelligence of the Coast Guard.
>
> (L) Such other elements of any other department or agency as may be designated by the President, or designated jointly by the Director of National Intelligence and the head of the department or agency concerned, as an element of the intelligence community.

[178] *See also* S. 4051 (111th Cong.) (identical to current version except that it included jurisdiction over aiders and abettors of violations of the provision enforcing secrecy obligations, at least where such violations occurred overseas).

Guidelines with respect to the new provision to take into consideration a number of factors relevant to the nature and scope of the offending disclosures.

H.R. 1823, the Criminal Code Modernization and Simplification Act of 2011, would overhaul the Espionage Act along with the rest of title 18, U.S. Code. Chapter 15, subchapter E of the proposed criminal code would replace the Espionage Act with three sections. Section 302 would prohibit the gathering of defense information or its transmission to any person not entitled to receive it, if done with the intent or reason to believe it "will be used to the injury of the United States, or to the advantage of any foreign power." Section 303 would apply only to those having lawful possession or control of defense information, providing for punishment of not more than 10 years' imprisonment in the event they recklessly permit it to be lost, stolen, or destroyed, or fail to report such an eventuality to an appropriate superior officer. Section 304 would prohibit the knowing disclosure of classified or similarly protected information to a person not entitled to receive it, or the use of such information to the injury of the United States or the advantage of a foreign power. Protected information would include restricted data under the Atomic Energy Act or information designated by the U.S. government as restricted on the basis of some relationship to cryptographic systems or communications intelligence, in substance as defined under current 18 U.S.C. Section 798. The proposed language eliminates any reference to specific items containing defense information or to specific means of acquiring or disseminating it, but otherwise appears to track the current law. The substitution of "foreign power" (as defined in the Foreign Intelligence Surveillance Act) for "foreign government" is perhaps the most noteworthy change from the Espionage Act as currently in force.

Two measures have been introduced to address recent newspaper reports alleged to contain sensitive intelligence information. The House of Representatives included a provision in the National Defense Authorization Act for FY2013 (H.R. 4310), passed by the House on May 18, 2012, to require the Attorney General to initiate within 30 days after enactment an investigation into possible violations of federal law regarding the disclosure of "sensitive information involving the military, intelligence, and operational capabilities of the United States and Israel," and to report on the status of the investigation no later than 60 days after enactment, Section 1099C. A resolution was introduced in the Senate to express the sense of the Senate that the Attorney General should delegate the task of investigating recent leaks of "classified and highly sensitive information related to various United States military and intelligence plans, programs, and operations" to an outside special counsel independent of the Department of Justice.

Conclusion

The Espionage Act on its face applies to the receipt and unauthorized dissemination of national defense information, which has been interpreted broadly to cover closely held government materials related to U.S. military operations, facilities, and personnel. It has been interpreted to cover the activities of foreign nationals overseas, at least when they take an active part in seeking out information. Although cases involving disclosures of classified information to the press have been rare, it seems clear that courts have regarded such disclosures by government employees to be conduct that enjoys no First Amendment protection, regardless of the motives of the divulger or the value the release of such information might impart to public discourse.[179] The Supreme

[179] The courts have permitted government agencies to enjoin their employees and former employees from publishing information they learned on the job, United States v. Marchetti, 466 F.2d 1309 (4th Cir.), *cert. denied*, 409 U.S. 1063 (continued...)

Court has stated, however, that the question remains open whether the publication of unlawfully obtained information by the media can be punished consistent with the First Amendment. Thus, although unlawful acquisition of information might be subject to criminal prosecution with few First Amendment implications, the publication of that information remains protected. Whether the publication of national security information can be punished likely turns on the value of the information to the public weighed against the likelihood of identifiable harm to the national security, arguably a more difficult case for prosecutors to make.

Author Contact Information

Jennifer K. Elsea
Legislative Attorney
jelsea@crs.loc.gov, 7-5466

(...continued)

(1972), and permitted harsh sanctions against employees who publish even unclassified information in violation of an obligation to obtain prepublication clearance, Snepp v. United States, 444 U.S. 507 (1980).