Criminal Prohibitions on Leaks and Other Disclosures of Classified Defense Information

Updated March 7, 2017

Congressional Research Service
https://crsreports.congress.gov
R41404

CRS REPORT
Prepared for Members and
Committees of Congress

Summary

Recent unauthorized disclosures of information concerning activities in the White House, and the publication of large quantities of classified information by WikiLeaks and other organizations and news outlets, have prompted congressional interest in criminal prohibitions on disclosure of classified information. While some have described recent leaks of classified information as "illegal" and "criminal," there is no single statute that criminalizes any unauthorized disclosure of classified information. Instead, the legal framework is based on a complex and often overlapping set of statutes with provisions that differ depending on, among other factors, what information was disclosed, to whom it was given, and the intentions of the discloser. This report identifies statutory prohibitions that may be implicated by the unauthorized release of classified information, and it examines the elements necessary to secure a conviction under the Espionage Act and applicable statutes.

Historically, the Espionage Act and other relevant statutes have been used almost exclusively to prosecute (1) individuals with access to classified information (and a corresponding obligation to protect it) who make it available to foreign agents, and (2) foreign agents who obtain classified information unlawfully while present in the United States. While prosecutions appear to be on the rise, disclosures of classified information to the press have been punished as crimes less frequently, and the government has never prosecuted a traditional news organization for publishing classified information that it received as a result of a leak.

This report examines prosecutions of individuals who leak information to the press or policy organizations, such as lobbying groups and think tanks, as well as civil and criminal actions that have been brought against the recipients of leaked information—often the press. Because these cases implicate unique First Amendment concerns regarding freedom of speech and freedom of the press, the constitutional framework relevant to prosecutions and other legal proceedings filed as a result of leaked classified information is also analyzed in this report.

Lastly, this report provides a summary of previous legislative efforts to criminalize the unauthorized disclosure of classified information and to address potential gaps or ambiguities in current statutes.

Contents

Contacts

Recent unauthorized disclosures to the press concerning activities in the White House,[1] and the publication of large quantities of classified information by WikiLeaks and other organizations and news outlets,[2] has prompted congressional interest in criminal prohibitions on disclosure of classified information. While President Trump[3] and certain media outlets have described certain White House leaks as "criminal"[4] and "illegal,"[5] there is no single statute that criminalizes any unauthorized disclosure of classified information.[6] Instead, criminal prohibitions on unauthorized disclosure of classified information are based on a complex and often overlapping set of statutes with provisions that differ depending on, among other factors, what material was leaked, to whom it was given, and the intent of the discloser.[7]

The most recent large-scale unauthorized disclosure occurred on March 7, 2017, when WikiLeaks published a collection of what it claims is the "largest ever publication of confidential documents" from the Central Intelligence Agency (CIA).[8] This material, dubbed "Vault 7" by WikiLeaks, has been reported to expose classified information[9] concerning, among other things, the CIA's technical capabilities to bypass encryption on certain phone and messaging services, to use "smart" televisions as listening devices, and to engage in certain types of cyberattacks.[10] In a press release, WikiLeaks claimed that its source for the classified material "wishes to initiate a public debate about the security, creation, use, proliferation and democratic control of

[1] *See, e.g.*, Mark Hensch, *WH to Probe Leak of Trump's Australia, Mexico Calls*, THE HILL (Feb. 3, 2017), http://thehill.com/homenews/administration/317887-wh-to-probe-leak-of-trumps-australia-mexico-calls; Paul Farhi, *The Trump Administration has Sprung a Leak. Many of Them, In Fact*, WASH. POST (Feb. 5, 2017), https://www.washingtonpost.com/lifestyle/style/the-trump-administration-has-sprung-a-leak-many-of-them-in-fact/2017/02/05/a13fad24-ebe2-11e6-b4ff-ac2cf509efe5_story.html?utm_term=.ef045235e744.

[2] *See infra* § "Private Manning and WikiLeaks" and § "Edward Snowden, National Security Agency Data-Collection Programs." *See also* Ewen MacAskill, Sam Thielman, & Philip Oltermann, *WikiLeaks Publishes 'Biggest Ever Leak of Secret CIA Documents,"* GUARDIAN (Mar. 7, 2016), https://www.theguardian.com/media/2017/mar/07/wikileaks-publishes-biggest-ever-leak-of-secret-cia-documents-hacking-surveillance.

[3] President Donald J. Trump (@realDonaldTrump) (Feb. 16, 2017, 3:58 AM), https://twitter.com/realDonaldTrump/status/832197515248275456 ("Leaking, and even illegal classified leaking, has been a big problem in Washington for years. Failing @nytimes (and others) must apologize!").

[4] President Donald J. Trump, Feb. 16, 2017 Press Conference, *transcript available at* http://www.cnn.com/2017/02/16/politics/donald-trump-news-conference-transcript/ ("I've actually called the Justice Department to look into the leaks. Those are criminal leaks.").

[5] Jonathan S. Tobin, *Trump's Flaws Don't Justify Illegal Leaks*, NAT'L REV. ONLINE (Feb. 16, 2017), http://www.nationalreview.com/article/445011/.

[6] See infra § "Statutory Protection of Classified Information."

[7] Commentators frequently contrast the patchwork nature of U.S. law with the United Kingdom's Official Secrets Act, 1989, c. 6 (U.K.), which more broadly criminalizes the dissemination and retention of numerous classes of government information. *See, e.g.*, David E. Pozen, *The Leaky Leviathan: Why the Government Condemns and Condones Unlawful Disclosures of Information*, 127 HARV. L. REV. 512, 626 (2013); William E. Lee, *Deep Background: Journalists, Sources, and the Perils of Leaking*, 57 AM. U.L. REV. 1453, 1466-67 (2008).

[8] Press Release, Vault 7: CIA Hacking Tools Revealed, WIKILEAKS (last visited Mar. 7, 2017), https://wikileaks.org/ciav7p1/#PRESS [hereinafter, "Vault 7 Press Release"].

[9] Nicholas Weaver, *The CIA's No Good, Very Bad, Totally Awful Tuesday*, LAWFARE (Mar. 7, 2017), https://www.lawfareblog.com/cias-no-good-very-bad-totally-awful-tuesday ("Two documents have Top Secret markings, which suggest either a mishandling of classified information or that the attacker managed to compromise a Top Secret CIA internal network.").

[10] *See* MacAskill *et al*. *supra* note 2; Scott Shane, Mark Mazetti, & Matthew Rosenberg, *WikiLeaks Releases Trove of Alleged C.I.A. Documents*, N.Y. TIMES (Mar. 7, 2017), https://www.nytimes.com/2017/03/07/world/europe/wikileaks-cia-hacking.html?hp&action=click&pgtype=Homepage&clickSource=story-heading&module=first-column-region&region=top-news&WT.nav=top-news.

cyberweapons."[11] This latest disclosure has prompted renewed questions regarding the government's ability to prosecute WikiLeaks and its founder, Julian Assange, for their role in the publication of classified material.[12]

Historically, the criminal statutes prohibiting the disclosure of protected information have been used almost exclusively to prosecute (1) individuals with access to classified information (and a corresponding obligation to protect it) who make it available to foreign agents and (2) foreign agents who obtain classified information unlawfully while present in the United States. In recent years, however, government officials have utilized the Espionage Act and other relevant statutes to prosecute individuals for providing classified information to news outlets and other organizations, including WikiLeaks, even when the accused claims to have a salutary motive of influencing public opinion or exposing potentially useful information about government programs. These prosecutions and the related proceedings that have been filed against members of the press who receive leaked information implicate unique constitutional considerations concerning the scope of First Amendment rights to freedom of speech and freedom of the press.[13]

Statutory Protection of Classified Information

While there is no single 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, the purpose of disclosure, and the means by which the information was obtained.[14] One broad category of information—national defense information—is protected by the Espionage Act,[15] while other types of relevant information are covered elsewhere in various provisions of the *U.S. Code*.[16] Some provisions apply only to government employees or others who have authorized access to sensitive government information,[17] but many apply to all persons.[18] Analysis of which statutory authorities are applicable to an unauthorized disclosure of classified information is likely to depend on the precise circumstances of the disclosure.[19]

[11] Vault 7 Press Release, *supra* note 8.

[12] *See* Seung Min Kim, *Sasse to DOJ, Should Assange be in Prison?* POLITICO (Mar. 9, 2017), http://www.politico.com/story/2017/03/ben-sasse-julian-assange-justice-department-235901.

[13] *See* U.S. CONST. amend. I ("Congress shall make no law ... abridging the freedom of speech, or of the press[.]").

[14] *See* sources cited *supra* note 7.

[15] Espionage Act of 1917, Ch. 30, 40 Stat. 217 (codified as amended, at 18 U.S.C. §§793-798).

[16] *See infra* § "Other Relevant Statutes."

[17] *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).

[18] *E.g.*, 18 U.S.C. §§793, 794, 798.

[19] *See, e.g.*, Harold Edgar & Benno C. Schmidt, Jr., *The Espionage Statutes and Publication of Defense Information*, 73 COLUM. L. REV. 929, 938-39 (1973) (identifying "major questions" must be answered before determining which statutory provisions may apply to the unauthorized disclosure of information: (1) the type of revelation or communication at issue, (2) the state of mind (or intent) of the person disclosing the information, and (3) the nature of the information that was communicated).

The Espionage Act

Originally enacted upon the United States' entry into World War I,[20] the Espionage Act is one of the U.S. government's primary statutory vehicles for addressing the disclosure of classified information.[21] The act is now codified as amended, in relevant part, in 18 U.S.C. Sections 793-798.[22] Each section provides for criminal prohibitions on gathering, handling, or transmitting information or other material "relating to the national defense"[23]—commonly referred to as *national defense information*[24]—and other protected classes of documents, material, or information defined by statute.[25]

The Espionage Act does not expressly address what constitutes information that is sufficiently related to national defense to fall within its ambit. However, in a 1941 decision, *Gorin v. United States*,[26] the Supreme Court explained that "national defense" is a "generic concept of broad connotations, relating to the military and naval establishments and the related activities of national preparedness."[27] While it is not necessary that a government agency mark information as classified in order for it to be protected under the Espionage Act, courts seem to give deference to the executive determination of what constitutes national defense information.[28] The act has been challenged on several occasions under the theory that the term *national defense information* is

[20] *See* Stephen I. Vladeck, *Inchoate Liability and the Espionage Act: The Statutory Framework and the Freedom of the Press*, 1 HARV. L. & POL'Y REV. 219, 221 (2007). For much of the nation's history prior to World War I, disclosure of government secrets was prosecuted under more generally applicable statutes punishing treason, entry onto military bases, and theft of government property. United States v. Rosen, 445 F. Supp. 2d 602, 611 (E.D. Va. 2006) (citing Edgar & Schdmidt, *supra* note 19, at 940).

[21] *See, e.g.*, Margaret B. Kwoka, *Leaking and Legitimacy*, 48 U.C. DAVIS. L. REV. 1387, 1413-14 (2015); Pozen, *supra* note 7, at 554. For more discussion of legal issues and interpretation related to the Espionage Act, see Fern L. Kletter, *Validity, Construction, and Application of the Federal Espionage Act, §§793 to 794*, 59 A.L.R. Fed. 2d 303 (2016).

[22] 18 U.S.C. §799, which was enacted as part of the National Aeronautics and Space Act of 1958, P.L. §85-568 §302(c), 72 Stat. 426, 434, is also included in the Espionage and Censorship chapter of the U.S. Code. This provision criminalizes certain violations of National Aeronautics and Space Administration (NASA) regulations related to protection or security of certain facilities, aircraft, spacecraft, and other property. *See* 18 U.S.C. §799.

[23] The statutes address "information respecting the national defense[,]" "information relating to the national defense[,]" and certain documents, maps, and other physical items "connected with the national defense[.]" 18 U.S.C. §§973(a)-(e); §794(a).

[24] *See, e.g.*, United States v. Rosen, 445 F. Supp. 2d 602, 607 (E.D. Va. 2006); United States v. Safford, 40 C.M.R. 528, 532 (A.C.M.R. 1969); William E. Lee, *Probing Secrets: The Press and Inchoate Liability for Newsgathering Crimes*, 36 AM. J. CRIM. L. 129, 168 (2009).

[25] Although the Espionage Act is divided into discrete sections, observers have noted that its provisions can be seen as overlapping. *See, e.g.*, Vladeck, *supra* note 20, at 222. Over the years, courts and commentators have criticized the Espionage Act as "excessively, complex, confusing, indeed impenetrable." *Rosen*, 445 F. Supp. 2d at 613 (citing various judicial opinions and scholarly commentaries).

[26] 312 U.S. 19 (1941).

[27] *Id.* at 28.

[28] The government must demonstrate that disclosure of a document is at least "potentially damaging" to the United States or advantageous to a foreign government. *See* United States v. Morison, 844 F.2d 1057, 1073 (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. At least one judge has held that in the case of a disclosure of intangible information, the government needs to prove only that the defendant has reason to believe that such information is potentially damaging, which, in the case of a person with access to classified information, can largely be inferred from the fact that information is classified. *See* United States v. Kiriakou, 898 F.Supp. 2d 921, 922 (E.D. Va. 2012) (scienter requirement heightened in the case of disclosure of intangible national defense information); *id.* at 925 (noting that defendant was a "government employee trained in the classification system who could appreciate the significance of the information he allegedly disclosed").

unconstitutionally vague and overbroad,[29] but the *Gorin* Court held that the mental state or mens rea requirements in the act, discussed below,[30] had a "delimiting" effect that gave what were otherwise potentially problematic terms sufficient definitiveness to pass constitutional muster.[31]

Section 793: General Protection of National Defense Information

The first provision of the Espionage Act, 18 U.S.C. Section 793, prohibits certain activities related to gathering, receiving, or transmitting national defense information to "one not entitled to receive it."[32] Section 793(a) prohibits obtaining information concerning a series of national defense installations (i.e., physical places) "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[.]"[33] Similarly, Section 793(b) prohibits individuals with "like intent or reason to believe" from obtaining or duplicating any "sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, document, writing, or note of anything connected with the national defense."[34]

Subsection (c) of Section 793 creates criminal liability for an individual who "receives or obtains, or agrees or attempts to receive or obtain" certain material related to national defense when the individual knows or has reason to believe that the material has been or will be "obtained, taken, made, or disposed of by any person contrary to the provisions of the [Espionage Act]."[35] Thus, whereas subsections (a) and (b) criminalize *collecting or copying* national defense information, subsection (c) prohibits its *receipt* so long as the recipient has (or should have) knowledge that the source violated another provision of the Espionage Act in the course of obtaining the information.[36]

---

[29] *See, e.g.*, *Gorin*, 312 U.S. at 23; *Morison*, 844 F.2d at 1063.

[30] *See infra* § "Mens Rea Requirements."

[31] *Gorin*, 312 U.S. at 27-28.

[32] 18 U.S.C. §793.

[33] 18 U.S.C. §793(a) creates criminal penalties for:

> (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....

[34] 18 U.S.C. §793(b) (emphasis added). The full subsection criminalizes:

> 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....

[35] 18 U.S.C. §793(c) creates criminal penalties for:

> (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 document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note, of anything 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*.]....

[36] *Compare* 18 U.S.C. §793(a)-(b) *with id.* §793(c). *See also* Vladeck, *supra* note 20, at 222-23.

Subsections (d) and (f) of Section 793 prohibit the dissemination of certain material and information relating to the national defense that is in the *lawful* possession of the individual who disseminates it. Subsection (d) prohibits willful dissemination,[37] and subsection (f) prohibits dissemination or mishandling through gross negligence.[38] Subsection (f) also applies when the lawful possessor of national defense information "fails to make prompt report" of its loss or theft.[39] When an individual has *unauthorized* possession of certain material or information related to the national defense, Section 793(e) prohibits its willful disclosure.[40]

Violators of any provision in Section 793 are subject to a fine or up to 10 years of imprisonment, or both,[41] as are those who conspire to violate the statute.[42]

Section 794: "Classic Spying" Cases

18 U.S.C. Section 794 covers so-called "classic spying" cases in which a defendant gathers or delivers national defense information or materials for use by foreign governments.[43] More specifically, Section 794 penalizes anyone who transmits information or certain material related to the national defense to a foreign government or foreign political or military party with the

[37] 18 U.S.C. §793(d) creates criminal penalties for the following:

> Whoever, lawfully having possession of, access to, control over, or being entrusted with any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note relating to the national defense, 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 or causes to be communicated, delivered, or transmitted or attempts to communicate, deliver, transmit or cause to be communicated, delivered or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it on demand to the officer or employee of the United States entitled to receive it[.]

[38] 18 U.S.C. §793(f) criminalizes:

> Whoever, being entrusted with or having lawful possession or control of any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, note, or information, relating to the national defense, (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 his 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[.]

[39] *Id.*

[40] 18 U.S.C. §793(e) creates penalties for:

> Whoever having unauthorized possession of, access to, or control over any document [or other protected thing related to the national defense], 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[.]

[41] 18 U.S.C. §793(f).

[42] 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.

[43] United States v. Morison, 844 F.2d 1057, 1065 (4th Cir.), *cert. denied*, 488 U.S. (1988) ("Manifestly, section 794 is a far more serious offense than section 793(d); it covers the act of 'classic spying'; and, because of its seriousness, it authorizes a far more serious punishment than that provided for section 793(d).").

intent or reason to believe it will be used to the injury of the United States or the advantage of a foreign nation.[44] Section 794 thus differs in primary respect from Section 793 in that it focuses on a more limited category of recipients—agents of foreign governments.[45] Section 794(b), which is applicable only "in time of war," further prohibits attempts to elicit information related to the public defense "which might be useful to the enemy[.]"[46] Subsection (c) makes it a crime to conspire to violate the provisions of Section 794.[47]

A violation of Section 794 is punishable by imprisonment for any term of years or life, or under certain circumstances, by a sentence of death.[48] The death penalty is available 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.[49] The death penalty is also available 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 reaches the enemy.[50] Offenders are also subject to forfeiture of any ill-gotten gains and property used to facilitate the offense.[51] In sum, Section 794 treats the transmission of national security information with intent to aid the enemy or a foreign government more severely than other types of disclosures.[52]

Sections 795-797: Images of Defense Installations and Equipment

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[53] and 797.[54] Similarly, Section 796 prohibits the use of an aircraft for the purpose of

[44] 18 U.S.C. §794.

[45] *See Morison*, 844 F.2d at 1065 ("The two statutes differ—and this is the critical point to note in analyzing the two statutes—in their identification of the person to whom disclosure is prohibited.").

[46] *Id.* §794(b).

[47] *Id.* §794(c).

[48] *Id.* §794(a)-(b).

[49] *Id.* §794(a) ("[T]he sentence of death shall not be imposed unless ... the offense resulted in the identification by a foreign power ... 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.").

[50] *See id.* §794(b). In addition, 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.

[51] 18 U.S.C. §794(d).

[52] *Compare id.* §794 *with id.* §793(h). *Accord* Mary-Rose Papandrea, *National Security Information and the Role of Intent*, 56 WM. & MARY L. REV. 1381, 1382-83 (2015).

[53] 18 U.S.C. §795 provides:

> (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....

[54] 18 U.S.C. §797 prohibits the publication and sale of photographs of defense installations, and provides that:

> On and after thirty days from the date upon which the President defines any vital military or naval

capturing images of a vital defense installation or equipment.[55] Violators are subject to fine or imprisonment for not more than one year, or both.[56]

Section 798: Certain Classified Information and Cryptographic Systems

18 U.S.C. Section 798 provides that the knowing and willful disclosure of certain specified types of classified information (as opposed to national defense information) is punishable by fine and/or imprisonment for not more than 10 years.[57] The provision applies only to certain categories of classified information, such as information concerning codes, ciphers, cryptographic systems, or other communications intelligence activities.[58] And the term "classified information" is limited to information that was classified "for reasons of national security[.]"[59] 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.[60]

Criminal Prohibitions Under the Uniform Code of Military Justice

Members of the military[61] who commit espionage akin 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

---

> 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.

[55] *See* 18 U.S.C. §796 (Prohibiting "the use of an aircraft or any contrivance used, or designed for navigation or flight in the air, for the purpose of making a photograph, sketch, picture, drawing, map, or graphical representation of vital military or naval installations or equipment[.]").

[56] *Id.* §§795-797.

[57] 18 U.S.C. §798 states:

> (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.

[58] *Id.* §798(a-b).

[59] *Id.* §7998(b).

[60] *Id.* §7998(a).

[61] 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.

Military Justice (UCMJ)[62] and sentenced to death if certain aggravating factors are found by unanimous determination.[63] 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."[64]

However, the government is not limited to charging the offense of espionage under Article 106a. Members could also be tried by court-martial for violations of Article 92, failure to obey order or regulation;[65] Article 104, aiding the enemy;[66] or under the general article, Article 134.[67] 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"[68] 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.

Other Relevant Statutes

In addition to the Espionage Act and its UCMJ counterparts, other criminal prohibitions in the *U.S. Code* have been or potentially could be utilized to prosecute the disclosure of classified information. 18 U.S.C. Section 1030(a)(1) punishes the willful retention, communication, or

---

10 U.S.C. §802.

[62] 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.

[63] 10 U.S.C. §906a(b)-(c).

[64] *Id.* §906a(c).

[65] *Id.* §892.

[66] *Id.* §904.

[67] *Id.* §934.

[68] *Id.*

transmission 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."[69] 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.[70] 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.[71] Repeat offenses or attempts can incur a prison sentence of up to 20 years.[72]

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 expressly prohibit disclosure of classified information, it has been used to prosecute "leakers."[73] 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.[74] It does not appear to have been used to prosecute any recipients of classified information even when the original discloser was charged under the statute.

The Intelligence Identities Protection Act, 50 U.S.C. Section 3121, provides for the protection of information concerning the identity of covert intelligence agents.[75] It generally covers persons authorized to know the identity of such agents or who learn the identity of covert agents as a

[69] 18 U.S.C. §1030(a)(1).

[70] 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.

[71] 10 U.S.C. §1030(c).

[72] *Id.* §1030(c)(1)(B).

[73] *See* United States v. Morison, 844 F.2d 1057 (4th Cir. 1988), *cert. denied*, 488 U.S. 908 (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 Drug Enforcement Agency 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).

[74] 18 U.S.C. §641.

[75] The Intelligence Identities and Protection Act of 1982, codified at 50 U.S.C. §§3121-26. 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. §3126(4)(c). "Intelligence agency" is defined as elements of the intelligence community, to include some offices within the Department of Defense, and intelligence elements of the Army, Navy, Air Force, Marine Corps, and Coast Guard; informant means "any individual who furnishes information to an intelligence agency in the course of a confidential relationship protecting the identity of such individual from public disclosure." 50 U.S.C. §3126(5-6). The definitions may suggest that the act is intended to protect the identities of persons who provide intelligence information directly to a military counterintelligence unit, but perhaps could 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. §3124.

result of their general access to classified information,[76] but can also apply to a person who learns of the identity of a covert agent through a "pattern of activities intended to identify and expose covert agents" and discloses the identity to any individual not authorized to access classified information with reason to believe that such disclosures would impair U.S. foreign intelligence efforts.[77] For those without authorized access, the crime is subject to a fine or imprisonment for a term of not more than three years.[78] 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.[79] To date, there have been no reported cases interpreting the statute, but two convictions pursuant to guilty pleas have resulted from the statute.[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 of 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]

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, for materials obtained during transmission from U.S. diplomatic missions abroad to the State Department or vice versa.[84] The

[76] Persons with direct access to information regarding the identities are subject to a prison term of not more than 15 years, while those who learn the identities through general access to classified information are subject to a term not greater than 10 years. 50 U.S.C. §3121. 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. §3122(b).

[77] 50 U.S.C. §3121.

[78] *Id.* §3121(c).

[79] *Id.* §3121(a)-(c).

[80] *See* Richard B. Schmitt, *Rare Statute Figures in Rove Case*, L.A. 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); Charlie Savage, *Former C.I.A. Operative Pleads Guilty in Leak of Colleague's Name*, N.Y. TIMES, October 23, 2012 (John Kiriakou pleaded guilty to disclosing a colleague's name to a journalist).

[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.

[84] Such transmissions may still be covered by the prohibition if the material was, or purports to have been, prepared

removal of classified material concerning foreign relations with the intent to store it at an unauthorized location is a misdemeanor under 18 U.S.C. Section 1924, which also applies only to U.S. government employees.[85]

50 U.S.C. Section 783 penalizes government officers or employees who, without proper authority, communicate classified information to a person who the employee has reason to suspect is an agent or representative of a foreign government.[86] It is also unlawful for the representative or agent of the foreign government to receive classified information.[87] Violation of either of these provisions is punishable by a fine of up to $10,000 or imprisonment for not more than 10 years.[88] Violators are thereafter prohibited from holding federal public office.[89] 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.[90]

The Atomic Energy Act of 1954, 42 U.S.C. Section 2274, prohibits disclosure of information relating to nuclear energy and weapons. The act creates criminal penalties for anyone who "communicates, transmits, or discloses" documents or information "involving or incorporating Restricted Data" with the "intent to injure the United States" or advantage a foreign nation,[91] or who has "reason to believe such data" would have that effect.[92]

Finally, 18 U.S.C. Section 2381 creates a criminal prohibition on treason punishable by death, imprisonment, or fine.[93] The statute applies when a person "owing allegiance to the United

---

using an official diplomatic code. It is unclear whether messages that are encrypted for transmission are covered.

[85] *See* 18 U.S.C. §1924(a).

[86] 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.

[87] 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.

[88] 50 U.S.C. §783(c).

[89] *Id.*

[90] 50 U.S.C. §783(e).

[91] 42 U.S.C. §2274.

[92] *Id.* §2274(b).

[93] 18 U.S.C. §2381. The treason statute is predicated on Article III, Section 3 of the Constitution, which states:

States" levies war against the country or gives its enemies "aid and comfort"[94]—a term which has been interpreted to include transmitting information to foreign agents.[95]

Mens Rea Requirements

One of the principal—and most complex—distinguishing factors among statutory prohibitions on the disclosure of protected information, particularly among the various sections of the Espionage Act, is the use of differing mens rea requirements.[96] Latin for "guilty mind," the term *mens rea* refers to the defendant's mental state of culpability that the government must prove in order to secure a conviction.[97] For instance, some laws require that the prosecution demonstrates that the defendant *intentionally* committed the act in question—that is, committed the act with the conscious desire for the harmful conduct to occur—while others require that the act be done with a lesser mens rea (e.g., willfully, knowingly, or negligently).[98]

Mens Rea and the Espionage Act

Sections 793(a-c) and 794 of the Espionage Act require the defendant to have acted with "*intent or reason to believe*" that the national defense information at issue "*is to be* used to the injury of the United States, or to the advantage of any foreign nation[.]"[99] In *Gorin*, the Supreme Court concluded that this provision requires the defendant to have acted in bad faith against the United States.[100]

Sections 793(d-e) and 798 contain dual mens rea elements in certain cases: the defendant must have (1) acted *willfully* in the act of disclosing the information and (2) with *reason to believe* the information *could be* used to injure the United States or to advantage a foreign nation.[101] The Supreme Court has described the "willful" standard in the criminal context as generally requiring

> Treason against the United States, shall consist only in levying war against them, or in adhering to their enemies giving them aid and comfort. No person shall be convicted of treason unless on the testimony of two witnesses to the same overt act, or on confession in open court.

[94] 18 U.S.C. §2381.

[95] *See* Chandler v. United States, 171 F.2d 921, 941 (1st Cir. 1948) (affirming conviction of defendant convicted of treason predicated on his radio broadcasting within the German Reich during World War II); United States v. Greathouse, 26 F. Cas. 18, 24 (C.C.N.D. Cal. 1863) ("[I]f a letter containing important intelligence for the insurgents be forwarded, the aid and comfort are given, though the letter be intercepted on its way.").

[96] For more background on *mens rea* requirements in federal criminal law, see CRS Report R44464, *Mens Rea Reform: A Brief Overview*, by Richard M. Thompson II. For scholarly treatment of the complex intent requirements in applicable statutes, see Papandrea, *supra* note 52.

[97] Black's Law Dictionary (10th ed. 2014) ("The state of mind that the prosecution, to secure a conviction, must prove that a defendant had when committing a crime.").

[98] *See* CRS Report R44464, *Mens Rea Reform: A Brief Overview*, *supra* note 96, at 1. *See also* Model Penal Code §2.02 (defining "Kinds of Culpability").

[99] 18 U.S.C. §§793(a-c); 794(a).

[100] United States v. Gorin, 312 U.S. 19, 27 (1941).

[101] At least one court has read these two elements together to require that the prosecution must prove that the defendant disclosed the information "with a bad faith purpose to either harm the United States or to aid a foreign government." United States v. Rosen, 445 F. Supp. 2d 602, 626 (E.D. Va. 2006). Later courts confronting the intent issue have differentiated this case to conclude that the "reason to believe" standard does not require an intent to do harm. *See* United States v. Drake, 818 F. Supp. 2d 909, 916 (D. Md. 2011) (distinguishing intent requirements between disclosures involving tangible documents and those involving intangible information); United States v. Kiriakou, 898 F. Supp. 2d 921, 924-27 (E.D. Va. 2012) (surveying case law and noting that a Fourth Circuit interlocutory appeal, United States v. Rosen, 557 F.3d 192, 194 (4th Cir. 2009), cast doubt on the district judge's interpretation).

that the accused was aware her conduct violated the law.[102] But, further adding to the complexity of the Espionage Act, the second prong of the mens rea requirements under Sections 793(d-e) does not apply to the disclosure of national-security-related documents and other physical material—only national security *information*.[103] Consequently, an additional burden of proof may be imposed when an individual communicates information to an unauthorized source rather than disclosing the document or other tangible material containing the information.[104]

Section 793(f) of the Espionage Act is unique in that it punishes the loss or removal of national defense information resulting from "gross negligence."[105] This standard has been described in other contexts as "the failure to exercise even a slight degree of care."[106] Prosecutions under the gross negligence provision of 18 U.S.C. Section 793(f) appear to be rare,[107] but at least two servicemembers were convicted under this provision, as applied through the UMCJ, for removing classified materials from a government workplace and failing to report or return the material upon discovering it had been removed.[108]

Other Mens Rea Requirements

Apart from the Espionage Act, 18 U.S.C. Section 1924 punishes the *knowing* removal of classified information by a government employee or contractor, with the intent to retain the information in an unauthorized location. A "knowing" mens rea generally requires the defendant

[102] *See* Bryan v. United States, 524 U.S. 184, 192 (1998); Ratzlaf v. United States, 510 U.S. 135 (1994). *See also* United States v. Morison, 844 F.2d 1057, 1071 (4th Cir. 1998), *cert denied*, 488 U.S. 908 (1988); United States v. Truong Dinh Hung, 629 F.2d 908, 919 (4th Cir. 1980).

[103] 18 U.S.C. §793(d-e) prohibit disclosure of national defense information when the possessor has reason to believe the information "could be used to the injury of the United States or to the advantage of any foreign nation[,]" but they do not apply the same "reason to believe requirement" to the disclosure of documents and other physical items. *See* New York Times Company v. United States, 403 U.S. 713, 738 n. 9 (1971) (White, J. concurring); United States. v. Drake, 818 F. Supp. 2d 909, 916-18 (D. Md. 2011); *Kiriakou*, 898 F. Supp. 2d at 923. In other provisions of the Espionage Act, the same standards apply to disclosure of information and physical material. *E.g.* 18 U.S.C. §793(f).

[104] *See*, *e.g.*, *Drake*, 818 F. Supp. 2d at 920-21 (distinguishing requirements for conviction under the Espionage Act when a "whistleblower" contacts the press about information that is believed to be of national concern versus when an individual retains a classified document relating to the national defense).

[105] 18 U.S.C. §793(f) (providing for criminal penalties for "[w]hoever, being entrusted with or having lawful possession or control of any document, writing, code book ... or information, relating to the national defense, (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[.]").

[106] Conway v. O'Brien, 312 U.S. 492, 495 (1941) (quoting Shaw v. Moore, 104 Vt. 529, 531 (1932)).

[107] Although there have been at least three charges under 18 U.S.C. §793(f) for unlawful transmission or retention of national defense information since January 1, 2000, CRS was able to identify only one charge under the gross negligence provision of this section. That charge was made against former FBI Agent James Smith, who was suspected of supplying classified information to a Chinese national over the course of a 20-year period. *See* Indictment, United States v. Smith, No. CR-03-4290M (C.D. Cal. May 7, 2003); Vincent J. Schodolski, Ex-FBI Agent Indicted in China Spy Case, CHI. TRIBUNE (May 8, 2003), http://articles.chicagotribune.com/2003-05-08/news/0305080212_1_katrina-leung-los-angeles-fbi-chinese-fugitive. Smith ultimately pled guilty to the lesser charge of making false statements under 18 U.S.C. §1001.

[108] *See* United States v. Gonzalez, 16 M.J. 428, 429 (C.M.A. 1983) (defendant "intermingled two classified messages with personal mail" which he removed from work before traveling to a friend's home where he left the materials in a desk drawer); United States v. Roller, 42 M.J. 264, 265 (C.A.A.F. 1995) (upon leaving his position at the Intelligence Division of the United States Marine Corps Headquarters, defendant placed classified material in a gym bag containing his personal effects and did not report the misplaced documents upon discovering them). For potential distinguishing characteristics between prosecutions for gross negligence under the UCMJ versus prosecutions against civilians, see John Ford, *Why Intent, Not Gross Negligence, is the Standard in Clinton Case*, WAR ON THE ROCKS (July 14, 2016), https://warontherocks.com/2016/07/why-intent-not-gross-negligence-is-the-standard-in-clinton-case/.

to have been aware that his conduct amounted to criminal behavior.[109] Other prohibitions on the disclosure of protected information incorporate the knowing standard either in conjunction with other mens rea requirements[110] or standing alone.[111]

In some cases, the available punishment depends on the defendant's mental state. For example, under the Atomic Energy Act of 1954, those who disclose documents or information with "intent" to advantage a foreign nation or harm the United States face possible life imprisonment and a $100,000 fine, but those who act with a "reason to believe" information could advantage a foreign nation face a maximum of 10 years in jail and a $50,000 fine.[112] Separate provisions apply when government employees, contractors, or military officials disclose restricted information identified in the Atomic Energy Act.[113]

Although some modern statutes create what are known as strict liability offenses that require no mens rea at all,[114] no current statutes appear to impose strict liability for the unauthorized disclosure or mishandling of classified information.

The First Amendment Framework

The publication of information pertaining to the national defense or foreign policy may serve the public interest by providing citizens with information that sheds light on the workings of government, but it seems widely accepted that the public release of at least some of this information poses a significant enough threat to national security 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 "provid[ing] for the common defense."[115] Policymakers are faced with the task of balancing these interests within the framework created by the Constitution.

The First Amendment to the U.S. Constitution provides that "Congress shall make no law ... abridging the freedom of speech, or of the press[.]"[116] Where speech is restricted based on its content, the Supreme Court generally applies "strict scrutiny," meaning 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."[117] The Supreme Court has described protection of the nation's security from external threat as a classic example of a compelling

[109] *See* Elonis v. United States, 135 S. Ct. 2001, 2011 (2015) (quoting Staples v. United States, 511 U.S. 600, 607 (U.S. 1994)) ("knowing" standard generally requires "awareness of some wrongdoing").

[110] *See* 50 U.S.C. §3121 (prohibiting the *intentional* disclosure of information identifying a covert agent while *knowing* that the information disclosed identifies the covert agent and the United States is taking affirmative measures to conceal the agent's status).

[111] *See* 50 U.S.C. §783 (penalizing government officers or employees who, without proper authority, communicate classified information to a person who the employee "knows or has reason to believe" is an agent or representative of a foreign government).

[112] 42 U.S.C. §2274(a-b).

[113] *See id.* §2277.

[114] Liability, Black's Law Dictionary (10th ed. 2014).

[115] U.S. CONST., pmbl.

[116] *Id.*, amend. I. 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.

[117] Sable Commc'ns of Cal. v. Fed. Commc'ns Comm'n, 492 U.S. 115, 126 (1989).

government interest.[118] 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.[119] Speech likely to incite immediate violence, for example, may be suppressed.[120] Speech that would give military advantage to a foreign enemy is also susceptible to government regulation.[121]

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 to cause damage to the national defense or foreign relations of the United States.[122] Actual damage need not be proved, but potential damage must be more than merely speculative and incidental.[123] On the other hand, the Court has stated that "state action to punish the publication of truthful information seldom can satisfy constitutional standards."[124] And it has described the constitutional purpose behind the guarantee of press freedom as the protection of "the free discussion of governmental affairs."[125]

---

[118] *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 (1964); *accord* Cole v. Young, 351 U.S. 536, 546 (1956)).

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

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

[121] 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.").

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

[123] *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); *see generally* 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)).

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

[125] 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 likely an implausible argument to posit that the First Amendment 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 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 organizations like WikiLeaks are not typical newsgathering and publishing companies 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).

Although information properly classified in accordance with statute or executive order, if disclosed to a person not authorized to receive it, carries by definition the potential of causing at least identifiable harm to the national security of the United States,[126] 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 be "closely held."[127] 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.[128] Typically, courts have been unwilling to review decisions of the executive related to national security, or have relied on a strong presumption that the material at issue is potentially damaging.[129] Still, judges have recognized that the government must make *some* showing that the release of specific national defense information has the potential to harm U.S. interests, lest the Espionage Act become a means to punish whistleblowers who reveal information that poses more of a danger of embarrassing public officials than of endangering national security.[130]

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 courts have not held that government classification of material is sufficient to show that its release is damaging to national security,[131] courts seem 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 such information poses no danger to U.S. national security would be persuasive without some convincing evidence to that effect or proof that the information is not closely guarded by the government.[132]

---

[126] Exec. Order No. 13526, 75 Fed. Reg. 707 §1.2 (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.

[127] 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).

[128] *See, e.g.*, United States v. Abu-Jihaad, 600 F.Supp.2d 362, 385-86 (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).

[129] *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.").

[130] *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), *cert. denied*, 488 U.S. 908 (1988).

[131] *See, e.g.*, Scarbeck v. United States, 317 F.2d 546 (D.C. Cir. 1962) (holding that 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).

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

Prosecution of Leaks and Disclosures to the Press

Although the criminal statutes prohibiting the disclosure of protected information have historically been used to prosecute individuals who made protected information available to foreign governments or against the agents of foreign governments themselves, courts have held that the Espionage Act is not limited to such "classic spying" cases involving foreign governments.[133] In some cases, criminal defendants have been successfully prosecuted even when claiming to have an altruistic desire to expose—i.e., leak[134]—potentially important information regarding government activities to the press or public policy advocacy organizations. And while there have been cases in which the government has been unable to secure convictions or has dropped or significantly reduced criminal charges against alleged leakers,[135] no individual has ever been acquitted based on a finding that the public interest in the released information was so great that it justified an otherwise unlawful disclosure. The following section discusses notable criminal prosecutions, both successful and unsuccessful, for leaks to the press or policy advocacy groups.[136]

The Criminal Prosecution for the Pentagon Papers Leak

The first notable instance of a prosecution for leaked information occurred in 1971 when two analysts at the Rand Corporation, Daniel Ellsberg and Anthony Russo, were indicted for disclosing a classified study prepared by the Department of Defense, which came to be known as the Pentagon Papers, on the role of the United States in the Vietnam War.[137] Ellsberg claimed he orchestrated the leak in an effort to influence public opinion and help bring about an end to the Vietnam War.[138] In addition to filing a civil action to block the *New York Times* and *Washington Post* from publishing the Pentagon Papers, discussed below,[139] the government brought criminal charges against Ellsberg and Russo for violations of Section 793 of the Espionage Act, conversion of government property, and conspiracy.[140] After more than two months of trial, revelations of government misconduct—including undisclosed wiretaps, a government-ordered break-in at Ellsberg's psychiatrist's office, and destruction of evidence—led the court to order a mistrial and the prosecution to drop its charges.[141]

---

[133] *See, e.g.*, United States v. Morison, 844 F.2d 1063-70 (4th Cir. 1988), *cert. denied*, 488 U.S. 908 (1988); United States v. Rosen, 445 F. Supp. 2d 602, 627-29 (E.D. Va. 2006).

[134] For a discussion of various definitions of the term "leak," see Pozen, *supra* note 7, at 521.

[135] For example, the charges against the individuals allegedly responsible for the Pentagon Papers leak were dropped following evidence of government misconduct. *See infra* § "The Criminal Prosecution for the Pentagon Papers Leak." And the charges against Thomas Drake were reduced after it was discovered that much of the information disclosed had been previously made public. *See infra* § "Thomas Drake, NSA Disclosures to the *Baltimore Sun*."

[136] For an analysis of high-profile leak incidents that includes individuals who were not prosecuted, see Yochai Benkler, *A Public Accountability Defense for National Security Leakers and Whistleblowers*, 8 HARV. L. & POL'Y Rev. 281, 311-20 (2014).

[137] For background on and access to the Pentagon Papers as published by the National Archives, see *Pentagon Papers*, NATIONAL ARCHIVES (Aug. 15, 2016), https://www.archives.gov/research/pentagon-papers.

[138] *See generally* DANIEL ELLSBERG, SECRETS: A MEMOIR OF VIETNAM AND THE PENTAGON PAPERS (2002).

[139] *See infra* "The Civil Litigation in the *Pentagon Papers* Case."

[140] Ellsberg and Russo were charged with violating 18 U.S.C. §§371, 641, 793(c), (d), (e). *See* United States v. Russo, No. 9373-(WMB)-CD (filed Dec. 29, 1971), dismissed (C.D. Cal. May 11, 1973); Stephen I. Vladeck, *Prosecuting Leaks under U.S. Law*, in WHISTLEBLOWERS, LEAKS, AND THE MEDIA: THE FIRST AMENDMENT AND NATIONAL SECURITY, 31 (Paul Rosenzweig et al., American Bar Association, 2014).

[141] For further background on the history of the case and the court's decision to declare a mistrial, see Melville B.

Samuel Loring Morison and *Jane's Defence Weekly*

In 1985, Samuel Loring Morison became the first person to be convicted for selling classified documents to the media, and the litigation arising from his prosecution, *United States v. Morison*, remains an important opinion on the requirements for conviction under the Espionage Act.[142] Charged with violating Section 793 of the Espionage Act and converting government property by providing classified satellite photographs of a Soviet naval vessel to the British defense periodical *Jane's Defence Weekly*, Morison argued that he lacked the requisite intent to commit espionage because he transmitted the photographs to a news organization and not to an agent of a foreign power.[143] The U.S. Court of Appeals for the Fourth Circuit rejected his appeal, finding the intent to sell photographs that he clearly knew to be classified sufficient to satisfy the mens rea requirement under 18 U.S.C. Section 793(d), which prohibits disclosure by a lawful possessor of defense information to one not entitled to receive it.[144] Morison's claim of a salutary motive—he argued that publication of the photos would show the gravity of the threat posed by the Soviet Union and spur public demand for an increased defense budget[145]—was not found to negate the element of intent.[146]

The fact that the Morison prosecution involved a leak to the media, with seemingly no obvious intent to transmit sensitive information to hostile intelligence services, did not persuade the jury, nor the courts, involved that he lacked culpability. The Justice Department did, however, come under some criticism on the basis that such prosecutions are so rare as to amount to a selective prosecution in his case, raising concerns about the chilling effect such prosecutions could have on would-be whistleblowers who could provide information embarrassing to the government but vital to public discourse.[147] On leaving office, President Clinton pardoned Morison.[148]

Lawrence Franklin and the AIPAC Disclosure

In 2005, Lawrence Franklin, a defense analyst at the Office of the Secretary of the Department of Defense, was indicted for disclosing classified information regarding American forces in Iraq to an Israeli diplomat and two employees of the American Israel Public Affairs Committee (AIPAC),

---

Nimmer, *National Security Secrets v. Free Speech: The Issues Left Undecided in the Ellsberg Case*, 26 STAN. L. REV. 311 (1974); Martin Arnold, *Pentagon Papers Charges are Dismissed; Judge Byrne Frees Ellsberg and Russo, Assails 'Improper Government Conduct'*, N.Y. TIMES, May 12, 1973, at A1, *available at* http://www.nytimes.com/learning/general/onthisday/big/0511.html#article.

[142] United States v. Morison, 844 F.2d 1057 (4th Cir. 1988), *cert. denied*, 488 U.S. 908 (1988).

[143] *Morison*, 844 F.2d at 1061-63.

[144] *Id.* at 1080.

[145] *Id.* at 1062. The government countered that his motive was to receive cash and employment from *Jane's Defence Weekly*. *Id.* at 1084-85 (Wilkinson, J., concurring). *See also* P. Weiss, *The Quiet Coup: U.S. v. Morison - A Victory for Secret Government*, HARPER'S, Sep. 1989.

[146] *Morison*, 844 F. 2d at 1073-74.

[147] *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), http://www.hks.harvard.edu/presspol/publications/papers/working_papers/2003_01_nelson.pdf; Ben A. Franklin, *Morison Receives 2-Year Jail Term*, N.Y. TIMES, Dec. 5, 1985, at A1 (noting criticism of the prosecution as a threat to freedom of the press).

[148] 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 from Sen. Daniel Patrick Moynihan to President Clinton (Sep. 29, 1998), *available at* http://www.fas.org/sgp/news/2001/04/moynihan.html.

a lobbying group focused on U.S.-Israel relations.[149] Franklin claimed he disclosed the information because he believed the threat to American security posed by Iran required more attention from officials in the National Security Council,[150] but he ultimately pled guilty to one count under the Espionage Act and one count of conspiracy to communicate classified information to an agent of a foreign government.[151] Franklin's case garnered significant attention when the government brought—and later dropped—charges against the AIPAC lobbyists who were on the receiving end of the leak, discussed below.[152]

Shamai Leibowitz, Leaked Transcripts of Calls with the Israeli Embassy

The first prosecution for unauthorized disclosure to the media during the Obama Administration occurred in 2009 against Shamai Leibowitz, a Hebrew translator working on contract for the FBI.[153] The government accused Leibowitz of disclosing classified information to a blogger in violation of Section 798 of the Espionage Act, but it never publicly identified the exact information disclosed or the identity of the blogger.[154] Media outlets reported that Leibowitz disclosed transcripts of conversations caught on FBI wiretaps of the Israeli Embassy in Washington, D.C.[155] Leibowitz claimed that his intention was to expose official misconduct, not damage national security,[156] but he ultimately pled guilty and was sentenced to 20 months in prison.[157]

Thomas Drake, NSA Disclosures to the *Baltimore Sun*

In April 2010, following an investigation that began during the George W. Bush Administration, a grand jury indicted a senior official at the National Security Agency (NSA), Thomas Drake,[158] on 10 felony charges for providing classified information regarding perceived mismanagement of NSA programs to the *Baltimore Sun*.[159] Drake's original indictment included five counts under the Espionage Act,[160] but the prosecution's case suffered setbacks after it was revealed that much

[149] For further detail on the AIPAC disclosure, see Lee, *supra* note 24, at 167-75.

[150] See *id*. at 167; Eric Lichtblau, *Pentagon Analyst Admits He Shared Secret Information*, N.Y. TIMES, Oct. 6, 2015, at A21.

[151] United States v. Rosen, 557 F.3d 192, 194 n.1 (4th Cir. 2009).

[152] *See infra* § "Criminal Prosecution of AIPAC Lobbyists in *United States v. Rosen*."

[153] Scott Shane, *Leak Offers Look at Efforts by U.S. to Spy on Israel*, N.Y. TIMES (Sep. 5, 2011), http://www.nytimes.com/2011/09/06/us/06leak.html?_r=2&hp=&pagewanted=all&.

[154] *See* Indictment of Shamai Leibowitz at 1, United States v. Leibowitz, No. AW09CR0632 (D. Md. Dec. 4, 2009), *available at* https://perma.cc/X559-4APF?type=pdf; Leonard Downie, Jr. & Sara Rafsky, *The Obama Administration and the Press: Leak Investigations and Surveillance in post-9/11 America*, COMM. TO PROTECT JOURNALISTS (Oct. 10, 2013), https://perma.cc/D4YG-X6Q3?type=source. The district judge presiding over the case was reported to have stated: "All I know is that it's a serious case. I don't know what was divulged other than some documents, and how it compromised things, I have no idea." Shane, *supra* note 153.

[155] Scott Shane, *Leak Offers Look at Efforts by U.S. to Spy on Israel*, N.Y. TIMES (Sep. 5, 2011), http://www.nytimes.com/2011/09/06/us/06leak.html?_r=2&hp=&pagewanted=all&.

[156] *See* Steven Aftergood, *Jail Sentence Imposed in Leak Case* (May 25, 2010), SECRECY NEWS, https://fas.org/blogs/secrecy/2010/05/jail_leak/.

[157] *Id.*; Vladeck, *supra* note 140, at 31.

[158] David Wise, *Leaks and the Law: The Story of Thomas Drake*, SMITHSONIAN MAGAZINE, Aug. 2011, *available at* http://www.smithsonianmag.com/history/leaks-and-the-law-the-story-of-thomas-drake-14796786/.

[159] Indictment of Thomas Drake, United States v. Drake, No. R0B18CR0181 (D. Md. Apr. 14, 2010), *available at* https://assets.documentcloud.org/documents/323707/drake-indictment.pdf.

[160] *Id.*

of the information at issue was either not classified or had been publicly discussed by other government officials,[161] and the court 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.[162] Drake eventually pled guilty to a single misdemeanor for exceeding his authorized use of an NSA computer.[163] Prior to issuing its sentence of one year probation and 240 hours of community service, the court called the government's treatment of Drake in the case "unconscionable," and it declined to impose a fine.[164]

Jeffrey Sterling, CIA Disclosures to *New York Times* Reporter James Risen

In a second investigation that began during the George W. Bush Administration and was carried into the Obama Administration, former CIA officer Jeffrey Sterling was indicted on December 22, 2010, for disclosing classified information about a covert CIA operation in which flawed nuclear blueprints were provided to Iran through a Russian scientist.[165] Sterling disclosed information about the program, which became known as "Operation Merlin," to *New York Times* reporter James Risen, who discussed it in a 2006 book about the CIA.[166] While some believe Sterling acted as a whistleblower about the dangers of Operation Merlin, especially because he raised concerns about the operation to the Senate Intelligence Committee, a jury found Sterling guilty on nine felony counts, including violations of the Espionage Act.[167] He was sentenced to 42 months in prison.[168]

Stephen Jim-Woo Kim, State Department Disclosure to Fox News Correspondent James Rosen

A State Department contract analyst, Stephen Jin-Woo Kim, was indicted in August 2010 for disclosing classified information about North Korea's plans to escalate its nuclear program to Fox News correspondent James Rosen.[169] Kim faced one count of violating the Espionage Act and one

[161] *Ex-Official for N.S.A. Accepts Deal in Leak Case*, N.Y. TIMES (June 10, 2011), http://www.nytimes.com/2011/06/11/us/11justice.html; Downie & Rafsky, *supra* note 154.

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

[163] *See* sources cited *supra* note 161.

[164] *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.

[165] *See* United States v. Sterling, 724 F.3d 482, 488 (4th Cir. 2013), *reh'g en banc denied*, 732 F.3d 292, *cert denied*, 134 S. Ct. 2696 (2014) ; In re Grand Jury Subpoena to Risen, No. 1:10CR485, 2010 U.S. Dist. LEXIS 143340, *1-3 (E.D. Va. Nov. 30, 2010); Indictment of Jeffrey Sterling, United States v. Sterling, No. 1:10CR485 (LMB) (E.D. Va. Dec. 22, 2010), *available* at https://assets.documentcloud.org/documents/323711/sterling-indictment.pdf [hereinafter, "Sterling Indictment"].

[166] *See* JAMES RISEN, STATE OF WAR: THE SECRET HISTORY OF THE CIA AND THE BUSH ADMINISTRATION 193-218 (2006).

[167] *See* Mark Apuzzo, *Ex-C.I.A. Officer Sentenced in Leak Case Tied to Times Reporter*, N.Y. TIMES (May 11, 2015), https://www.nytimes.com/2015/05/12/us/ex-cia-officer-sentenced-in-leak-case-tied-to-times-reporter.html; Steven Nelson, *Jeffrey Sterling Sentenced to 42 Months for Talking to Reporter*, U.S. NEWS & WORLD REPORT (May 11, 2015), https://www.usnews.com/news/articles/2015/05/11/jeffrey-sterling-sentenced-to-42-months-for-talking-to-reporter.

[168] *See* sources cited *supra* note 167.

[169] *See* United States v. Jin-Woo Kim, 808 F. Supp. 2d 44, 47 (D.D.C. 2011); Ann E. Marimow, *Ex-State Department Adviser Stephen J. Kim Sentenced to 13 Months in Leak Case*, WASH. POST (Apr. 2, 2014), https://perma.cc/2QBB-36K9?type=source.

count of making false statements to the FBI.[170] After the court denied his motions to dismiss the espionage charges based on the Constitution's Treason Clause as well as the First and Fifth Amendments,[171] Kim pled guilty to a single count of disclosing national defense information to a person not authorized to receive it in violation of Section 793(d) of the Espionage Act.[172] He was sentenced to 13 months in prison.[173]

Private Manning and WikiLeaks

While serving as an Army intelligence analyst in Baghdad, Private First Class Chelsea (formerly Bradley) Manning downloaded more than 250,000 U.S. State Department diplomatic cables, video footage of an airstrike that resulted in the deaths of civilians, and other classified material from the government's Secret Internet Protocol Router Network (SIPRNET) system.[174] When materials were eventually disseminated and published through WikiLeaks, military officials charged Manning with numerous violations of the UCMJ, including aiding the enemy under UCMJ Article 104—a crime that carries a potential for capital punishment or life imprisonment[175]—and violating the Espionage Act as applied through Article 134 of the UCMJ.[176]

Manning pled guilty to 10 charges, including all Espionage Act counts, but prosecutors pursued the remaining charges against him without seeking the death penalty.[177] In 2013, Manning was convicted by court-martial of all charges except aiding the enemy, and was sentenced to 35 years of imprisonment, reduction in rank, forfeiture of pay, and a dishonorable discharge.[178] On January 17, 2017, President Obama commuted Manning's sentence, which now expires on May 17, 2017.[179]

In addition to the criminal prosecution of Manning, a grand jury empaneled in Alexandria, VA, investigated civilian involvement in the matter,[180] but information regarding the targets of the

[170] Jin-Woo Kim, 808 F. Supp. 2d at 47.

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

[172] Josh Gerstein, *Contractor Pleads Guilty in Leak Case*, POLITICO (Feb. 7, 2014), http://www.politico.com/story/2014/02/stephen-kim-james-risen-state-department-fox-news-103265; Letter from US. Dep't of Justice to Counsel for Stephen Jim-Woo Kim (Feb. 2, 2014), *available at* https://fas.org/sgp/jud/kim/plea.pdf.

[173] Marimox, *supra* note 169.

[174] *See* Tim Bakken, *The Prosecution of Newspapers, Reporters, and Sources for Disclosing Classified Information: The Government's Softening of the First Amendment*, 45 U. TOL. L. REV. 1, 18 (2013).

[175] 10 U.S.C. §904.

[176] 10 U.S.C. §934. *See also See* Ed Pilkington, *Bradley Manning May Face Death Penalty*, GUARDIAN (March 3, 2011), 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 12 specifications).

[177] *See* Bakken, *supra* note 174; Katherine Feuer, Article: *Protecting Government Secrets: A Comparison of the Espionage Act and the Official Secrets Act*, 38 B.C. INT'L & COMP. L. REV. 91, 104 (2015); Ed Pilkington, *Bradley Manning Pleads Guilty to 10 Charges But Denies 'Aiding the Enemy,'* GUARDIAN (Feb. 28, 2013), https://www.theguardian.com/world/2013/feb/28/bradley-manning-pleads-aiding-enemy-trial.

[178] Charlie Savage and Emmarie Huetteman, *Manning Sentenced to 35 Years for a Pivotal Leak of U.S. Files*, N.Y. TIMES, August 21, 2013, at A1.

[179] The White House, Office of the Press Secretary, *President Obama Grants Commutations and Pardons*, OBAMA WHITE HOUSE ARCHIVES (Jan. 17, 2017), https://obamawhitehouse.archives.gov/the-press-office/2017/01/17/president-obama-grants-commutations-and-pardons.

[180] The Department of Justice cited an ongoing investigation into the disclosures as a reason to deny a request for information under the Freedom of Information Act (FOIA). *See* Government Motion for Summary Judgment, Manning v. U.S. Dep't of Justice, No. 1:15-cv-01654 (D.D.C. March 15, 2016).

investigation and the prosecution's theory of the case remains under seal.[181] Although certain media outlets reported that WikiLeaks founder Julian Assange was the subject of a sealed indictment for his role in the disclosure,[182] U.S. officials denied that a sealed indictment had been filed,[183] and no public charges against Assange have been filed.

John Kirakou, Violation of the Intelligence Identities Protection Act

In April 2012, a grand jury indicted former CIA officer John Kirakou for charges arising from the alleged disclosure of classified information related to the CIA's detention and interrogation program to journalists.[184] Kirakou was indicted on five felony counts: three violations of the Espionage Act, one count of making false statements to federal officials, and one count of violating the Intelligence Identities Protection Act[185] for providing the name of a covert CIA operative to a reporter.[186] While Kirkaou argued that he had been singled out for prosecution because of his earlier public criticism of the CIA,[187] he pled guilty to violating the Intelligence Identities Protection Act,[188] in a case that was reported to have been the first conviction under that law in 27 years.[189] The remaining charges were dropped as part of his plea agreement, and he was sentenced to 30 months in prison.[190]

[181] Based on a letter accompanying a grand jury subpoena, there was 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 was reported that a conspiracy theory could permit prosecutors to pursue charges on the basis of activities not subject to First Amendment protection. *See* Scott Shane, *Supporter of Leak Suspect Is Called Before Grand Jury*, N.Y. TIMES, June 16, 2011, at 22 (quoting attorney Abbe D. Lowell).

[182] *See*, *e.g.*, Josh Gerstein, *Report: WikiLeaks' Founder Julian Assange Indicted in U.S.*, POLITICO (Feb. 28, 2012), http://www.politico.com/blogs/under-the-radar/2012/02/report-wikileaks-founder-julian-assange-indicted-in-us-115779; Philip Dorling, *Charges Against Assange Drawn Up in US, Says Email*, SYDNEY MORNING HERALD (Feb. 29, 2012).

[183] Sari Horwitz, *Assange Not Under Sealed Indictment, U.S. Officials Say*, WASH. POST (Nov. 18, 2013), https://www.washingtonpost.com/world/national-security/assange-not-under-sealed-indictment-us-officials-say/2013/11/18/8a3cb2da-506c-11e3-a7f0-b790929232e1_story.html?utm_term=.dd07d17e561e.

[184] *See* Indictment of John Kiriakou, United States v. Kiriakou, No. 1:12cr127 (LMB) (E.D. Va. Apr. 5, 2012). *See also* Vladeck, *supra* note 140, at 33.

[185] 50 U.S.C. §3121.

[186] See Dep't of Justice, Office of Public Affairs, Former CIA Officer John Kiriakou Indicted for Former CIA Officer John Kiriakou Indicted for Allegedly Disclosing Classified Information, Including Covert Officer's Identity, to Journalists and Lying to CIA's Publications Board, (Apr. 5, 2012), https://www.justice.gov/opa/pr/former-cia-officer-john-kiriakou-indicted-allegedly-disclosing-classified-information.

[187] *See CIA 'Whistleblower' John Kiriakous Jailed for Two Years for Identity Leak*, GUARDIAN (Oct. 23, 2012), https://www.theguardian.com/world/2012/oct/23/cia-whistleblower-john-kiriakou-leak.

[188] Dep't of Justice, U.S. Attorney's Office, *Former CIA Officer Sentenced to 30 Months for Revealing Identity of 20-Plus-Year Covert CIA Officer* (Jan. 25, 2013), https://www.justice.gov/usao-edva/pr/former-cia-officer-sentenced-30-months-revealing-identity-20-plus-year-covert-cia.

[189] Justin Jouvenal, *Former CIA Officer John Kiriakou is Sentenced to 30 Months in Prison for Leaks*, WASH. POST. (Jan. 25, 2013), https://www.washingtonpost.com/local/former-cia-officer-john-kiriakou-sentenced-to-30-months-in-prison-for-leaks/2013/01/25/49ea0cc0-6704-11e2-9e1b-07db1d2ccd5b_story.html?utm_term=.63797e7c6995.

[190] Dep't of Justice, U.S. Attorney's Office, *supra* note 188; Charlie Savage, *Former CIA Operative Pleads Guilty in Leak of Colleague's Name*, N.Y. TIMES, Oct. 24, 2012, at A16.

James Hitselberger, Navy Linguist Disclosure to the Hoover Institution

In May 2012, a grand jury indicted a former Navy contract linguist in Bahrain, James Hitselberger, on three counts of violating the Espionage Act and three counts of unlawful removal of a public record in violation of 18 U.S.C. Section 2071(a)[191] for providing certain classified information to the Hoover Institution,[192] a public policy think tank at Stanford University. Hitselberger, who claimed that his case was "overcharged,"[193] entered into a plea agreement in which all Espionage Act charges were dropped, and he pled guilty to a single misdemeanor count of unlawful removal of classified material under 18 U.S.C. Section 1924[194] for attempting to take certain classified materials outside of a secure work area.[195] He was sentenced to time served.[196]

Donald Sachtleben, Disclosure of Foiled Bomb Plot to the Associated Press

Donald Sachtleben, a former Special Agent Bomb Technician and then-contractor for the FBI, was charged with multiple counts of violating the Espionage Act in September 2013 for leaking classified information relating to a foiled suicide bombing attack on a U.S.-bound airliner by operatives of Al Qaeda in the Arabian Peninsula.[197] Although the government filings did not publicly identify the recipient of the information, it was widely reported that Sachtleben leaked the information to the Associated Press (AP).[198] The case garnered significant attention after it was made known that the government subpoenaed AP journalists' phone records for evidence against Sachtleben without advance notice to the targets of the subpoenas.[199] Sachtleben ultimately pled guilty to two counts of violating the Espionage Act and was sentenced to 43 month of imprisonment.[200]

---

[191] 18 U.S.C. §2071(a) states:

> Whoever willfully and unlawfully conceals, removes, mutilates, obliterates, or destroys, or attempts to do so, or, with intent to do so takes and carries away any record, proceeding, map, book, paper, document, or other thing, filed or deposited with any clerk or officer of any court of the United States, or in any public office, or with any judicial or public officer of the United States, shall be fined under this title or imprisoned not more than three years, or both.

[192] *See* Indictment, United States v. Hitselberger, No. 12-231 (D.D.C. filed Feb. 28, 2013); Vladeck, *supra* note 140, at 29 n.1. *See also* Josh Gerstein, Linguist Charged with Pilfering Records seeks Release, POLITICO (Dec. 4, 2012), http://www.politico.com/blogs/under-the-radar/2012/12/linguist-charged-with-pilfering-records-seeks-release-151097.

[193] Steven Aftergood, *Espionage Act Case was "Overcharged" Defense Says*, SECRECY NEWS (June 30, 2014), https://fas.org/blogs/secrecy/2014/06/esp-act-overcharged/.

[194] For a summary of this statute, see § "Other Relevant Statutes."

[195] *See* Judgment, United States v. Hitselberger, No. 12-231 (D.D.C. filed July 18, 2014); Superseding Information, United States v. Hitselberger, No. 12-231 (D.D.C. filed Apr. 25, 2014); Josh Gerstein, *Ex-Navy Linguist Pleads Guilty in Secret documents Case*, POLITICO (Apr. 25, 2014), http://www.politico.com/blogs/under-the-radar/2014/04/ex-navy-lingust-pleads-guilty-in-secret-documents-case-187436.

[196] *See* Judgment, United States v. Hitselberger, No. 12-231 (D.D.C. filed July 18, 2014).

[197] Statement of Offense, United States v. Sachtleben, No. 1:13-cr-0200 WTL-TAB (S.D. In. filed Sep. 23, 2014).

[198] *See*, *e.g.*, Josh Gerstein, *Ex-FBI Agent Admits to AP Leak*, POLITICO (Sep. 23, 2013), http://www.politico.com/story/2013/09/ex-fbi-agent-pleads-guilty-associated-press-leak-case-097226; Tim Evans, *Ex-FBI Bob Tech's High-Profile Career Ends in Scandal*, USA TODAY (Sep. 25, 2013), http://www.usatoday.com/story/news/nation/2013/09/25/fbi-bomb-tech-career-ends-in-scandal/2868499/.

[199] *See* Charlie Savage and Leslie Kaufman, *Phone Records of Journalists Seized by U.S.*, N.Y. TIMES, May 14, 2013, at A1; Sari Horwitz, *Justice Dept. Seized Phone Records of AP Journalists*, WASH. POST, May 14, 2013, at A1.

[200] *See* Dep't of Justice, U.S. Attorney's Office, *Former Federal Contractor Sentenced For Disclosing National Defense Information And Distributing Child Pornography* (Nov. 14, 2013), https://www.justice.gov/usao-sdin/pr/former-federal-contractor-sentenced-disclosing-national-defense-information-and. Sachtleben simultaneously entered

Edward Snowden, National Security Agency Data-Collection Programs

In 2013, Edward Snowden, a former contractor working as a computer systems administrator at an NSA facility in Hawaii, was charged in connection with leaking top-secret documents related to certain NSA data-collection programs[201] to the *Guardian* (UK) and the *Washington Post*.[202] Snowden permitted the newspapers to publish his name, but fled to Hong Kong before he could be taken into custody. Snowden reportedly sought asylum in Ecuador[203] but remains at large under a temporary residency permit in Russia.[204] A still-pending criminal complaint charges Snowden with violating Sections 793(d) and 798(a)(3) of the Espionage Act and theft of government property under 18 U.S.C. Section 641.[205] Russia is reported to have declined U.S. requests for extradition.[206]

Unauthorized Disclosure by General David Petraeus

Former Army General and Director of the CIA David Petraeus was charged with misdemeanor removal of documents and materials containing classified information with intent to retain them at an unauthorized location in violation of 18 U.S.C. Section 1924 in March 2015.[207] Petraeus was accused of disclosing classified information to an Army Reserve officer who was writing his biography and with whom Petraeus admitted to having been engaged in a romantic relationship.[208] Although his case does not fit the common mold for a leak prosecution because Petraeus did not disclose information to the press or another public policy organization as part of an alleged effort to influence public opinion, his case still received significant public attention given his senior role in the government.[209] Petraeus pled guilty to the misdemeanor charge, and

---

into a plea agreement and pled guilty to child pornography-related offenses uncovered in an unrelated investigation. *Id.*

[201] For background on changes to the NSA's telephony metadata program in the wake of the Snowden disclosures, see CRS Legal Sidebar WSLG794, *President Obama Announces Changes to NSA Telephony Metadata Program*, by Edward C. Liu.

[202] Mark Mazzetti and Michael S. Schmidt, *Ex-Worker at C.I.A. Says He Disclosed U.S. Surveillance*, N.Y. TIMES, June 10, 2013, at A1.

[203] Ellen Barry and Peter Baker, *Snowden, in Russia, Seeks Asylum in Ecuador*, N.Y. TIMES, June 23, 2013, at A1. However, Ecuador later backed away from accepting Snowden. Juan Forero, *Ecuador's Strange Journey from Embracing Snowden to Turning Him Away*, WASH. POST (July 2, 2013), https://www.washingtonpost.com/news/worldviews/wp/2013/07/02/ecuadors-strange-journey-from-embracing-snowden-to-turning-him-away/.

[204] Snowden was originally granted temporary asylum in Russia, but was given a three-year residency permit beginning on August 1, 2014. *See* Joe Sterling, Russia Gives Snowden 3-Year Residency, CNN (Aug. 7, 2014), http://www.cnn.com/2014/08/07/world/europe/russia-snowden-residency/.

[205] *See* Dep't of Justice, Office of Public Affairs, Justice Department Statement on the Request to Hong Kong for Edward Snowden's Provision Arrest (June 26, 2013), https://www.justice.gov/opa/pr/justice-department-statement-request-hong-kong-edward-snowden-s-provisional-arrest.

[206] *See* Tom McCarthy, *Putin Confirms Snowden in Moscow Airport but Denies Extradition – As It Happened*, GUARDIAN (June 25, 2013), https://www.theguardian.com/world/2013/jun/25/edward-snowden-russia; Brian Ross et al., *Vladimir Putin Defies U.S. on Edward Snowden Extradition*, ABC NEWS (June 25, 2013), http://abcnews.go.com/Blotter/edward-snowden-show-2nd-cuba-flight-russia-fires/story?id=19480761. For background on obstacles in the effort to extradite Snowden, see CRS Legal Sidebar WSLG561, *U.S. May Face Significant Obstacles in Attempt to Apprehend Edward Snowden*, by Michael John Garcia.

[207] Bill of Information, United States v. Petraeus, No. 3:15 CR 47, (W.D.N.C. Mar. 3, 2015), available at http://www.ncwd.uscourts.gov/sites/default/files/general/Petraeus.pdf.

[208] *See* Jonathan Allen, Josh Gerstein, & Jennifer Epstein, *Citing Affair, Petraeus Resigns at CIA*, POLITICO (Nov. 11, 2012), http://www.politico.com/story/2012/11/citing-affair-petraeus-resigns-at-cia-08364; Michael S. Schmidt and Matt Apuzzo, *F.B.I. and Justice Dept. Said to Seek Charges for Petraeus*, N.Y. TIMES, Jan. 10, 2015, at A1.

[209] *See, e.g.*, sources cited *supra* note 208; *Petraeus Sentenced to 2 Years Probation for Military Leak*, FOXNEWS (Apr. 23, 2015), http://www.foxnews.com/politics/2015/04/23/petraeus-sentenced-to-2-years-probation-for-military-

prosecutors recommended a $40,000 fine as part of a plea agreement,[210] but the court imposed the maximum $100,000 fine based on what it deemed to be the serious nature of the crime.[211]

Legal Proceedings Involving the Press or Other Recipients of Unlawful Disclosures

While courts have held that the Espionage Act and other relevant statutes allow for convictions for leaks *to* the press,[212] the government has never prosecuted a traditional news organization for its *receipt* of classified or other protected information.[213] The plain terms of the Espionage Act, however, do not focus solely on the initial disclosure of national defense information.[214] While there is some authority for interpreting portions of the Espionage Act as to exclude "publication" of material from the criminal provisions,[215] some have argued that the act could be read to apply to anyone who, while meeting applicable mens rea requirements, disseminates, distributes, receives, or retains national defense information or material, even if such actions are taken as a member of the press.[216]

On one occasion, the government pursued (but later dropped) Espionage Act charges against two AIPAC lobbyists for their alleged role in receiving and further distributing national security information leaked by a government employee.[217] And the role of the press in leak prosecutions became the subject of frequent discussion among legal and media commentators[218] following a series of cases in which the government sought to gather evidence from the media about their

leak.html; Adam Goldman, *Petraeus Pleads Guilty to Mishandling Classified Material, Will Face Probation*, WASH. POST. (Apr. 23, 2015), https://www.washingtonpost.com/world/national-security/petraeus-set-to-plead-guilty-to-mishandling-classified-materials/2015/04/22/3e6dbf20-e8f5-11e4-aae1-d642717d8afa_story.html?utm_term=.f1f319d378f7.

[210] *See* Plea Agreement, United States v. Petraeus, No. 3:15 CR 47, (W.D.N.C. Mar. 3, 2015), available at http://www.ncwd.uscourts.gov/sites/default/files/general/Petraeus.pdf.

[211] *See* Ken Otterbourg and Andrew Grossman, *Gen. David Petraeus Avoids Jail Time, to Pay $100,000 Fine*, WALL ST. J. (Apr. 23, 2015), https://www.wsj.com/articles/david-petraeus-sentenced-to-two-years-probation-1429816999.

[212] *See supra* § "Prosecution of Leaks and Disclosures to the Press."

[213] Papandrea, *supra* note 52, at 1389. *See also* Espionage Act and the Legal and Constitutional Issues Raised by WikiLeaks: Hearing Before the H. Comm. On the Judiciary, 111th Cong. 39-40, 43 (2010) [hereinafter, "House Judiciary WikiLeaks Hearing"] (statement of Kenneth L. Wainstein, former Assistant Attorney General, Partner, O'Melveny & Myers, LLP).

[214] *See, e.g.* 18 U.S.C. §793(a) (criminal prohibition on one who, with the required *mens rea*, "obtains" national defense information); *id.* §793(c) (criminal prohibition on an individual who "receives or obtains or agrees or attempts to receive or obtain" certain national defense material); *id*. §793(f) (criminal prohibition on the "fail[ure] to make prompt report" of the loss, theft, abstraction, or destruction" of national defense information").

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

[216] *See, e.g.*, House Judiciary WikiLeaks Hearing, *supra* note 213, at 67 (statement of Stephen Vladeck) ("[T]he text of the [Espionage] Act makes no distinction between the leaker, the recipient of the leak, or the 100th person to redistribute, retransmit, or even retain national defense information that ... is already in the public domain."); *id.* Vladeck, *supra* note 20, at 231-32.

[217] *See infra* § "Criminal Prosecution of AIPAC Lobbyists in *United States v. Rosen*."

[218] *See, e.g.*, Vladeck, *supra* note 20, at 231-32; Lee, *supra* note 24, at 130-36; Dana Milbank, *In AP, Rosen Investigations, Government Makes Criminals of Reporters*, WASH. POST (May 21, 2013), http://articles.washingtonpost.com/2013-05-21/opinions/39419370_1_obama-administration-watergate-benghazi.

sources through secret subpoenas that were not made known to their targets. The following section discusses these notable legal proceedings in which members of the press or other recipients of leaked information were implicated in legal proceedings either as the subject of a civil or criminal suit itself or as the target of the government's effort to gather and present evidence.

Criminal Prosecution of AIPAC Lobbyists in *United States v. Rosen*

The only known instance of criminal prosecution against the recipient of classified information in the context of a leak occurred in the case of Lawrence Franklin's disclosure of classified material to two AIPAC lobbyists, discussed above.[219] The lobbyists, Steven J. Rosen and Keith Weissman, 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*.[220] Their part in the conspiracy included receiving information from government employees with knowledge that the employees were not authorized to disclose it and disclosing that information to others.[221] The prosecution was criticized for effectively "criminalizing the exchange of information,"[222] 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.[223]

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.[224] With respect to the intent requirement under the Espionage Act, the judge

[219] *See supra* § "Lawrence Franklin and the AIPAC Disclosure."

[220] United States v. Rosen, 445 F. Supp. 2d 602 (E.D. Va. 2006) (Rosen and Weissman were charged with conspiracy under 18 U.S.C. §793(g) to violate 18 U.S.C. §793 (d) & (e); Rosen was additionally charged with another violation of 18 U.S.C. §793(d)); *see* 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). During World War II government officials considered prosecuting the Chicago Tribune for publishing a story which suggested that the United States won the Battle of Midway because it was able to read Japanese codes. *See* Mary-Rose, Papandrea, *Lapdogs, Watchdogs, and Scapegoats: The Press and National Security Information*, 83 IND. L.J. 233, 258 (2008). When Japan did not change its coded communications, the Department of War asked the Department of Justice to drop the matter so as not to draw attention to the United States' intelligence capabilities. *See id.*; Geoffrey R. Stone, *Freedom of the Press in Time of War*, 59 SMU L. REV. 1663, 1668 (2006); House Judiciary WikiLeaks Hearing, *supra* note 213, at 61 (statement of Gabriel Schoenfeld).

[221] *Rosen*, 445 F. Supp. 2d at 608; *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").

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

[223] *See* Lee, *supra* note 24, at 132-34. The solicitation theory relied on a finding in a 2008 Supreme Court case, United States v. Williams, 553 U.S. 285 (2008), that solicitation of an illegal transaction is not speech deserving of First Amendment protection. *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* addressed 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*, 553 U.S. at 304.

[224] *See* Markon, *supra* note 114 (quoting Dana J. Boente, the then-Acting U.S. Attorney for the Eastern District of Virginia, 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." *Rosen*, 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,

interpreted the term "willfully" in connection with the phrase "reason to believe could be used to the injury of the United States" in Section 793 to require that the prosecution must prove that the defendant disclosed the information "with a bad faith purpose to either harm the United States or to aid a foreign government."[225] Later courts confronting the intent issue have differentiated this case to conclude that the "reason to believe" standard does not require the intent to do harm.[226]

The Civil Litigation in the *Pentagon Papers* Case

With regard to the issue of possible prosecutions of the press for publishing information leaked by a government employee, the most relevant case is likely to be the *Pentagon Papers* case.[227] In addition to the criminal prosecution of Daniel Ellsberg and Anthony Russo for disclosure of the Pentagon Papers, the Nixon Administration filed civil suits against the *New York Times* and *Washington Post*, seeking to prevent them from publishing the leaked documents.[228] The consolidated case quickly reached the Supreme Court,[229] which, in a terse per curiam opinion accompanied by a separate concurring or dissenting opinion by every member of the Court, rejected the government's request for a temporary restraining order and preliminary injunction barring publication.[230] Although the fact that the case concerned an injunction against publication in civil suits rather than a prosecution for publication is a significant distinguishing factor, the Supreme Court recognized a high level of First Amendment protection afforded to the press in the *Pentagon Papers* case. Its decision to deny the injunction may inform decisions involving criminal prosecutions of the press or other media organizations.[231]

The Supreme Court's *Pentagon Papers* decision does not, however, foreclose the possibility that a newspaper or other media outlet could be convicted of a criminal violation for publishing protected information. Several Justices suggested in separate dicta that the newspapers—along with the former government employee who leaked the documents to the press—could be criminally prosecuted under the Espionage Act even if an injunction was not available.[232] Still, in

1084 (4th Cir. 1988) (Wilkinson, J., concurring)).

[225] *Rosen*, 445 F. Supp. 2d at 625.

[226] *See* United States v. Drake, 818 F. Supp. 2d 909, 916 (D. Md. 2011) (distinguishing intent requirements between disclosures involving tangible documents and those involving intangible information); United States v. Kiriakou, 898 F. Supp. 2d 921, 924-27 (E.D. Va. 2012) (surveying case law and noting that a Fourth Circuit interlocutory appeal in the *Rosen* case cast doubt on the district judge's interpretation).

[227] N. Y. Times Co. v. United States, 403 U.S. 713 (1971) (per curiam).

[228] *See id.*

[229] The Department of Justice filed its first complaint against the New York Times on June 14, 1971, JAKE KOBRICK, THE PENTAGON PAPERS IN THE FEDERAL COURTS 2 (2014), and the Supreme Court issued its written opinion just over two weeks later on June 30, 1971. *See N.Y. Times*, 403 U.S. at 713.

[230] *See N.Y. Times*, 403 U.S. at 714.

[231] *See* Papandrea, *supra* note 52, at 1420-23 (discussing the impact and potential applicability of the *Pentagon Papers* case in criminal prosecutions for disclosure of protected information); House Judiciary WikiLeaks Hearing, *supra* note 213, at 20 (statement of Geffrey R. Stone) ("The standard applied in the Pentagon Papers case is *essentially* the same standard the Court would apply in a criminal prosecution of an organization or individual for publicly disseminating information about the conduct of government.") (emphasis in original).

[232] *See N.Y. Times Co.*, 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. 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).

a later case, the Court stressed that any prosecution of a publisher for what has already been printed would have to overcome only slightly less insurmountable hurdles.[233]

The publication of truthful information that is lawfully acquired enjoys considerable First Amendment protection.[234] 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."[235] (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.)

In other First Amendment cases, the Supreme Court has established that "routine newsgathering" is presumptively lawful acquisition, the fruits of which may be published without fear of government retribution.[236] However, what constitutes "routine newsgathering" has not been further elucidated. In a 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.[237] 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.[238]

Gathering Evidence from the Press

In most circumstances, no civil or criminal proceedings have been filed against members of the media that receive leaked information or documents during the course of their newsgathering activities, but there have been several cases in which legal disputes arose out of the government's efforts to obtain testimony or records from the members of the press as part of its prosecution of leakers.

In the trial of former CIA officer Jeffrey Sterling,[239] the Obama Administration sought to compel *New York Times* reporter James Risen to testify regarding classified information the prosecution believed Sterling had provided to Risen.[240] Following Risen's motion to quash the trial subpoena,

[233] 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.

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

[235] Fla. Star v. B.J.F. 491 U.S. 524, 535 n.8 (1989) (emphasis in original). The Court also questioned whether the receipt of information can ever constitutionally be proscribed. *Id.* at 536.

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

[237] Bartnicki v. Vopper, 532 U.S. 514 (2001).

[238] *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).

[239] *See supra* § "Jeffrey Sterling, CIA Disclosures to *New York Times* Reporter James Risen."

[240] *See* United States v. Sterling, 818 F. Supp. 2d 945 (E.D. Va. 2011) [hereinafter, "*Sterling I*"], *rev'd*, 724 F.3d 482 (4th Cir. 2013) [hereinafter, "*Sterling II*"], *reh'g en banc denied*, 732 F.3d 292, (4th Cir. 2013), *cert. denied*, 134 S. Ct. 2696 (2014).

the district court concluded that, under the First Amendment, there is a qualified reporter's privilege[241] that may be invoked when a subpoena seeks information about confidential sources or is intended to harass the journalist.[242] The district court limited the scope of Risen's testimony such that he was not compelled to reveal his confidential source.[243] On appeal, however, the U.S. Court of Appeals for the Fourth Circuit reversed the ruling, holding there is neither a First Amendment privilege nor a federal common-law privilege protecting journalists from being compelled to testify.[244] Despite prevailing on appeal, the government did not call Mr. Risen to testify at the jury trial.[245]

In the investigation of Donald Sachtleben over leaks of covert efforts to foil a bomb plot on a U.S.-bound airliner,[246] the Department of Justice was reported to have been unable to identify the source of the leaks until it issued subpoenas to obtain the calling records for 20 telephone lines associated with AP bureaus and reporters.[247] The targets of the subpoenas at the AP were not notified that their information was being collected, prompting criticism in the press of the government's evidence-gathering methods.[248]

Similarly, the case of former State Department contractor Stephen Jin-Woo Kim's disclosures to Fox News correspondent James Rosen generated attention when it was revealed that the Department of Justice subpoenaed Rosen's emails without notice.[249] In its application for the search warrant, the government characterized Rosen as having acted "much like an intelligence officer would run an [sic] clandestine intelligence source,"[250] and it asserted in a sworn statement that "there is probable cause to believe that the Reporter has committed a violation of 18 U.S.C. Sec. 793 (Unauthorized Disclosure of National Defense Information), at the very least, either as an aider, abettor, or co-conspirator of Mr. Kim."[251] Although Rosen was never charged with a crime in connection with his alleged receipt of classified information, the affidavit's language

---

[241] For an overview of the law regarding the reporter's privilege, see CRS Report RL34193, *Journalists' Privilege: Overview of the Law and Legislation in the 113th Congress*, by Kathleen Ann Ruane.

[242] *Sterling I*, 818 F. Supp. 2d at 951.

[243] *Id.* at 960.

[244] *Sterling II*, 724 F.3d at 504-05. For additional background and analysis of the Fourth Circuit's decision, see CRS Legal Sidebar WSLG630, *Confusing Branzburg: Is There a Journalists' Privilege Under the First Amendment?*, by Kathleen Ann Ruane.

[245] *See* Brief of Defendant-Appellant Jeffrey Alexander Sterling to the U.S. Court of Appeals for the Fourth Circuit, United States v. Sterling, No. 15-4297, filed Feb. 22, 2016, at 13, *available at* http://www.fas.org/sgp/jud/sterling.

[246] *See supra* § "Donald Sachtleben, Disclosure of Foiled Bomb Plot to the Associated Press."

[247] *See* Charlie Savage, *Former F.B.I. Agent to Plead Guilty in Press Leak*, N.Y. TIMES, Sep. 23, 2013, at A1. For further background and analysis of the AP subpoenas, see CRS Legal Sidebar WSLG517, *Reporter's Privilege and Department of Justice Access to Reporters' Phone Records*, by Kathleen Ann Ruane.

[248] *See*, *e.g.*, Milbank, *supra* note 218; Ravi Somaiua, *Head of the A.P. Criticizes Seizure of Phone Records*, N.Y. TIMES, May 20, 2013, at B8. *See also* Amitai Etzioni, *A Liberal Communitarian Approach to Security Limitations on the Freedom of the Press*, 22 WM. & MARY BILL RTS. J. 1141, 1143-44 (2014) (summarizing media reactions). *But see*, *e.g.*, Daniel J. Gallington, Editorial, *There Is No Scandal in Tracking Down Leaks*, U.S. NEWS & WORLD REP. (May 20, 2013), http://www.usnews.com/opinion/blogs/world-report/2013/05/20/obama-is-right-to-target-ap-national-security-leaks.

[249] See Affidavit in Support of Application for a Search Warrant, P 3, No. 10-291-M-01 (D. D.C. Nov. 7, 2011), available at http://apps.washingtonpost.com/g/page/local/affidavit-for-search-warrant/162/ n [hereinafter, "Rosen Warrant Affidavit"]; Charlie Savage, *Ex-Contractor at State Dept. Pleads Guilty in Leak Case*, N.Y. TIMES, Feb. 8, 2014, at A10. *See also* Amitai Etzioni, *A Liberal Communitarian Approach to Security Limitations on the Freedom of the Press*, 22 WM. & MARY BILL RTS. J. 1141, 1143-44 (2014).

[250] Rosen Warrant Affidavit, *supra* note 249, at ¶ 39(c).

[251] *Id.* ¶¶ 40. 248

suggesting he may be charged for violating the Espionage Act was met with considerable criticism in the press.[252] The backlash was reported to have contributed to the Department of Justice's decision to revise its policies for investigating leaks.[253] The new guidelines, issued in July 2013, provide that "members of the news media will not be subject to prosecution based solely on newsgathering activities."[254]

The Classified Information Protection Act of 2001

The current laws protecting classified information have been criticized by some as a patchwork of mostly outdated provisions that are vague and inconsistent,[255] or that may not cover all the information the government legitimately needs to protect.[256] Conversely, others argue that the laws fail to take due consideration of the value of releasing to the public information that the government would prefer to keep out of view.[257]

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

> 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.[258]

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.[259] In short, the provision would have made it a

---

[252] *See, e.g.*, Michael Calderone & Ryan J. Reilly, *DOJ Targeting of Fox News Reporter James Rosen Risks Criminalizing Journalism*, HUFFINGTON POST (May 20, 2013), http://www.huffingtonpost.com/2013/05/20/doj-fox-news-james-rosen_n_3307422.html; Milbank, *supra* note 218; Editorial, *Justice Department Run Amok on Journalists*, S.F. CHRON. (May 22, 2013), http://www.sfchronicle.com/opinion/editorials/article/Justice-Department-run-amok-on-journalists-4540632.php.

[253] *See* Savage, *supra* note 249.

[254] DEP'T OF JUSTICE, REPORT ON NEWS MEDIA POLICIES 2 (July 12, 2013), *available at* http://www.justice.gov/iso/opa/resources/2202013712162851796893.pdf.

[255] *See* sources cited *supra* note 25.

[256] *See, e.g.*, House Judiciary WikiLeaks Hearing, *supra* note 213.

[257] *See id*.

[258] 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.

[259] 18 U.S.C. §1924 prohibits removal of government-owned or controlled classified information by a government 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

crime to disclose or attempt to disclose classified information[260] 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 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 also 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,"[261] 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.[262] President Clinton, however, 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."[263] 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.[264]

The 107th Congress considered passing an identical provision,[265] 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 legislative or administrative actions.[266] An identical measure was introduced late in the 109th Congress, but was not reported out of committee.[267]

---

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.

[260] "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."

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

[262] H.R. 4392 §304, 106th Congress.

[263] 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).

[264] *Id*.

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

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

[267] S. 3774, 109th Cong.

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

> Although 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.[268]

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. Although cases involving disclosures of classified information to the press have not been common, 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.[269] The question remains open as to whether the publication of unlawfully obtained information by the media can be punished consistent with the First Amendment.[270] Thus, although unlawful acquisition of information might be subject to criminal prosecution with few First Amendment implications, the publication of that information may be protected. Whether the publication of national security information can be punished may turn on the value of the information to the public weighed against the likelihood of identifiable harm to national security, arguably a more difficult case for prosecutors to make.

Author Information

Stephen P. Mulligan
Legislative Attorney

Jennifer K. Elsea
Legislative Attorney

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

[269] 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. 1972), *cert. denied*, 409 U.S. 1063 (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).

[270] *See* § "The Civil Litigation in the *Pentagon Papers* Case."

Disclaimer