Congressional Research Service
Informing the legislative debate since 1914

Criminal Prohibitions on Leaks and Other Disclosures of Classified Defense Information

Updated May 11, 2023

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

CRS REPORT
Prepared for Members and
Committees of Congress

Congressional Research Service
Informing the legislative debate since 1914

SUMMARY

R41404

May 11, 2023

Stephen P. Mulligan
Legislative Attorney

Jennifer K. Elsea
Legislative Attorney

Criminal Prohibitions on Leaks and Other Disclosures of Classified Defense Information

High-profile leaks and disclosures of protected government information have prompted frequent congressional interest in the criminal penalties for disclosing government secrets. In one recent case, a U.S. Air National Guardsman allegedly posted photographs on social media of documents that, according to media outlets, contained classified information about the Russia-Ukraine war and other international affairs.

No single statute criminalizes all unauthorized disclosure of protected government information. Rather, the legal framework is based on a complex and often overlapping set of statutes or individual provisions within statutes, which are outlined in this report. Criminal prosecutions arising from unauthorized disclosures frequently focus on the Espionage Act, with specific charges varying based on certain factors. Successful prosecutions can result in punishments ranging from severe penalties and imprisonment for "classic spying" cases (when an individual collects information in an effort to provide aid to a foreign government) to less severe penalties for cases such as failing to report that protected information has been mishandled or lost.

Historically, the United States has prosecuted under the Espionage Act and related statutes (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. The United States has also prosecuted individuals claiming an altruistic desire to expose protected information to the public based on their belief that the public good favors transparency into particular government activities. While not every prosecution against an alleged "whistleblower" has been successful, no individual has been acquitted on the grounds that the public interest in the leaked information was so significant as to justify an otherwise unlawful disclosure.

Some have questioned whether the Espionage Act covers only initial disclosure of protected information or whether it also criminalizes the receipt and publication of that information by third parties, such as the press. The United States has never prosecuted a traditional news organization for receiving and publicizing leaked information, but it has extended its prosecution efforts to the individual not responsible for the initial disclosure. 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.

Prosecutions and legal proceedings arising out of leaks may also implicate First Amendment issues regarding freedom of speech and freedom of the press. At the same time, exposure of protected information may harm U.S. national security. Because these cases can raise 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, discussing ways Members of Congress who are evaluating criminal prohibitions on disclosures of protected information may seek to balance these competing interests within the constitutional framework.

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. Members may also consider past proposals for legislative changes to the Espionage Act.

Contents

Contacts

Leaks[1] and other unauthorized disclosures of protected government information have drawn recurring congressional interest to the criminal penalties for disclosing government secrets.[2] No single statute criminalizes all unauthorized disclosure of protected government information.[3] Rather, the legal framework is based on a complex and often overlapping set of statutes or individual provisions within statutes. Criminal prosecutions arising from unauthorized disclosures frequently focus on the Espionage Act, with specific charges varying based on factors such as what information was released, to whom it was given, and the discloser's intentions.[4] Charges against these individuals can range from serious offenses for "classic spying" cases (when an individual collects information to aid a foreign government) to less severe offenses, such as the failure to report that protected information has been mishandled or lost.[5]

Historically, the criminal statutes prohibiting the disclosure of protected information have been used largely 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.[6] In recent years, some prosecutors have brought charges against individuals under the Espionage Act and related statutes for providing classified information to news outlets and other organizations even when the accused "leaker" claimed to have a salutary motive of wanting to influence public opinion or expose potentially useful information about government programs.

This report examines U.S. statutes that create criminal penalties for disclosing classified and other protected government information. It discusses select high-profile prosecutions of individuals accused of disclosing information, including prosecutions for those who disclose such information to the press and other groups. Next, this report examines civil and criminal actions against the recipients of leaked information. Because these matters raise First Amendment questions regarding freedom of speech and freedom of the press, the constitutional framework

[1] U.S. law does not define *leak*, and there is no agreed-upon definition of the term in academic literature. This report uses *leak* in the colloquial sense to refer to intentional disclosures of protected government information by an individual inside or previously inside the government, such as an employee, former employee, or contractor to the media or the public by other means. For a discussion on the disagreement on the term's definition and scope, see David E. Pozen, *The Leaky Leviathan: Why the Government Condemns and Condones Unlawful Disclosures of Information*, 127 HARV. L. REV. 512, 521 (2013) (providing a "working definition" of *leak* as "(i) a targeted disclosure (ii) by a government insider (employee, former employee, contractor) (iii) to a member of the media (iv) of confidential information the divulgence of which is generally proscribed by law, policy, or convention (v) outside of any formal process (vi) with an expectation of anonymity"). The report does not address other unauthorized disclosures, such as providing classified information to a foreign agent.

[2] *See, e.g.*, Secrecy Orders and Prosecuting Leaks: Potential Legislative Responses to Deter Prosecutorial Abuse of Power, Hearing Before H. Comm. on the Judiciary, 117th Cong. (2021) [hereinafter Secrecy Orders Hearing]; Espionage Act and the Legal and Constitutional Issues Raised by WikiLeaks: Hearing Before the H. Comm. on the Judiciary, 111th Cong. (2010) [hereinafter House Judiciary WikiLeaks Hearing]; Media Leaks of Classified Information, Hearing Before H. Permanent Select Comm. on Intel., 109th Cong. (2006); Examining DOJ's Investigation of Journalists Who Publish Classified Information: Lessons from the Jack Anderson Case, Hearing Before S. Comm. on the Judiciary, 109th Cong. (2006); Espionage Laws and Leaks: Hearings Before H. Permanent Select Comm. on Intel., Subcomm. on Legis., 96th Cong. (1979).

[3] Commentators frequently contrast the varied set of U.S. laws with the United Kingdom's Official Secrets Act, 1989, c. 6 (UK), which more broadly criminalizes the dissemination and retention of numerous classes of government information. *See, e.g.*, William E. Lee, *Deep Background: Journalists, Sources, and the Perils of Leaking*, 57 AM. U.L. REV. 1453, 1466–67 (2008); Pozen, *supra* note 1**Error! Bookmark not defined.**, at 626.

[4] *See infra* §§ "The Espionage Act; Mens Rea Requirements."

[5] *Compare infra* § "The Espionage Act." *with infra* § "Mens Rea Requirements."

[6] *See, e.g.*, Pozen, *supra* note 1, at 554 ("The majority of Espionage Act prosecutions have, appropriately enough, involved espionage, incidents in which an official passed confidential information to a foreign power.").

relevant to prosecutions and other legal proceedings filed as a result of leaked information is also analyzed in this report. Lastly, this report summarizes a select set of legislative proposals to amend the Espionage Act and related statutes to address potential gaps or ambiguities in current law.

Statutory Protection of Classified Information

While there is no single statute that criminalizes the unauthorized disclosure of any classified information, a patchwork of statutes 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. One broad category of information—national defense information—is protected by the Espionage Act,[7] while other types of relevant information are covered elsewhere in various provisions of the *U.S. Code*.[8] Some provisions apply only to government employees or others who have authorized access to sensitive government information,[9] but many apply to all persons.[10] 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.[11]

The Espionage Act

Originally enacted upon the United States' entry into World War I,[12] the Espionage Act is one of the U.S. government's primary statutory vehicles for addressing the disclosure of classified information.[13] The act is now codified as amended, in relevant part, in 18 U.S.C. Sections 793–798.[14] Each section provides for criminal prohibitions on gathering, handling, or transmitting information or other material "relating to the national defense"[15]—commonly referred to as

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

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

[9] *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).

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

[11] *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).

[12] *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 11, at 940).

[13] *See, e.g.*, Margaret B. Kwoka, *Leaking and Legitimacy*, 48 U.C. DAVIS. L. REV. 1387, 1413–14 (2015); Pozen, *supra* note 1, 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).

[14] 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.

[15] 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).

national defense information[16]—and other protected classes of documents, material, or information defined by statute.[17]

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*, 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."[18] 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.[19] The act has been challenged on several occasions under the theory that the term *national defense information* is unconstitutionally vague and overbroad,[20] but the *Gorin* Court held that the mental state or mens rea requirements in the act, discussed below,[21] had a "delimiting" effect that gave what were otherwise potentially problematic terms sufficient definitiveness to pass constitutional muster.[22]

Section 793: General Protection of National Defense Information

The first provision of the Espionage Act, 18 U.S.C. § 793, prohibits certain activities related to gathering, receiving, or transmitting national defense information to one "not entitled to receive it."[23] 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."[24] 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."[25]

---

[16] *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).

[17] 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 12, 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).

[18] 312 U.S. 19, 28 (1941).

[19] 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. 1988), *cert. denied*, 488 U.S. 908 (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 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").

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

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

[22] *Gorin*, 312 U.S. at 27–28.

[23] 18 U.S.C. § 793.

[24] *Id.* § 793(a).

[25] 18 U.S.C. § 793(b).

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.[26] 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.[27]

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,[28] and subsection (f) prohibits dissemination or mishandling through gross negligence.[29] Subsection (f) also applies when the lawful possessor of national defense information "fails to make prompt report" of its loss or theft.[30] When an individual has *unauthorized* possession of certain material or information related to the national defense, Section 793(e) prohibits its willful disclosure.[31]

Violators of any provision in Section 793 are subject to a fine or up to ten years of imprisonment, or both,[32] as are those who conspire to violate the statute.[33]

Section 794: "Classic Spying" Cases

Section 794 of Title 18 covers "classic spying" cases in which a defendant gathers or delivers national defense information or materials for use by foreign governments.[34] More specifically, Section 794 penalizes anyone who transmits information or certain material related to the national defense to a foreign government, a foreign political party, or a foreign military party with the intent or reason to believe it will be used to the injury of the United States or the advantage of a foreign nation.[35] Section 794 thus primarily differs from Section 793 by focusing on a more limited category of recipients—agents of foreign governments.[36] 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.... "[37] Subsection (c) makes it a crime to conspire to violate the provisions of Section 794.[38]

---

[26] *Id.* 793(c).

[27] *Compare* 18 U.S.C. § 793(a)–(b) *with id.* § 793(c). *See also* Vladeck, *supra* note 12, at 222–23.

[28] 18 U.S.C. § 793(d).

[29] *Id.* § 793(f).

[30] *Id.*

[31] *Id.* § 793(e).

[32] *Id.* § 793(f).

[33] *Id.* § 793(g).

[34] United States v. Morison, 844 F.2d 1057, 1065 (4th Cir.), *cert. denied*, 488 U.S. 908 (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).").

[35] 18 U.S.C. § 794.

[36] *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.").

[37] *Id.* § 794(b).

[38] *Id.* § 794(c).

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.[39] The death penalty is available upon a finding that the offense resulted in the death of an agent of the United States or directly concerns nuclear weapons or other particularly sensitive types of information.[40] 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.[41] Offenders are also subject to forfeiture of any ill-gotten gains and property used to facilitate the offense.[42] 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.[43]

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. §§ 795 and 797.[44] Similarly, Section 796 prohibits the use of an aircraft for the purpose of capturing images of a vital defense installation or equipment.[45] Violators are subject to fine or imprisonment for not more than one year, or both.[46]

Section 798: Certain Classified Information and Cryptographic Systems

Section 798 of Title 18 provides that the knowing and willful disclosure of certain specified types of classified information (as opposed to national defense information) is punishable by fine, imprisonment for not more than ten years, or both.[47] The provision applies only to certain categories of classified information, such as information concerning codes, ciphers, cryptographic systems, or other communications intelligence activities.[48] The term *classified information* is limited to information that was classified "for reasons of national security."[49] 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.[50]

---

[39] *Id.* § 794(a)–(b).

[40] *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.").

[41] *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 103b 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. § 903b.

[42] 18 U.S.C. § 794(d).

[43] *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).

[44] 18 U.S.C. §§ 795, 797.

[45] *See Id.* § 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.").

[46] *Id.* §§ 795–797.

[47] *Id.* § 798.

[48] *Id.* § 798(a)–(b).

[49] *Id.* § 798(b).

[50] *Id.* § 798(a).

Criminal Prohibitions Under the Uniform Code of Military Justice

Members of the military[51] who commit espionage akin to the conduct prohibited under 18 U.S.C. § 794 may be tried by court-martial for violating Article 103a of the Uniform Code of Military Justice (UCMJ)[52] and sentenced to death if certain aggravating factors are found by unanimous determination.[53] Unlike offenses under Section 794, Article 103a 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 103a 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."[54]

However, the government is not limited to charging the offense of espionage under Article 103a. Members can also be tried by court-martial for violating Article 92, failure to obey order or regulation;[55] Article 103b, aiding the enemy;[56] or Article 134, the general article.[57] 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" that are not enumerated elsewhere in the UCMJ.[58] 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. § 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. § 1030(a)(1) punishes the willful retention, communication, or 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."[59] Receipt of information procured in violation of the statute is not addressed, but depending on the specific facts surrounding the unauthorized access, those who did not themselves access government computers may still be liable conspirators, aiders and abettors, or accessories after the fact.[60] The

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

[52] *Id.* § 903a(a).

[53] *Id.* § 903a(b)–(c).

[54] *Id.* § 903a(c).

[55] *Id.* § 892.

[56] *Id.* § 903b.

[57] *Id.* § 934.

[58] *Id.*

[59] 18 U.S.C. § 1030(a)(1).

[60] 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.

provision imposes a fine or imprisonment for not more than 10 years, or both, in the case of a first offense or attempted violation.[61] Repeat offenses or attempts can incur a prison sentence of up to twenty years.[62]

Section 641 of Title 18 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."[63] Violators may be fined, imprisoned for not more than 10 years, or both, unless the value of the property does not exceed $100, in which case the maximum prison term is one year.[64] 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.[65] To date, this section 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. § 3121, provides for the protection of information concerning the identity of covert intelligence agents.[66] It generally covers persons authorized to know the identity of such agents or who learn the identity of covert agents as a result of their general access to classified information,[67] 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.[68] For those without authorized access, the crime is subject to a fine or imprisonment for a term of not more than three years.[69] To be convicted, a violator must have knowledge that the

[61] 18 U.S.C. § 1030(c).

[62] *Id.* § 1030(c)(1)(B).

[63] *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, 310 (4th Cir. 1991) ("[I]nformation 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).

[64] 18 U.S.C. § 641.

[65] *Id.*

[66] The Intelligence Identities and Protection Act of 1982, 50 U.S.C. §§ 3121–26 (formerly codified at 50 U.S.C. §§ 421-426). 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." *Id.* § 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. *Id.* § 3124.

[67] Persons with direct access to information regarding the identities are subject to a prison term of not more than fifteen years, while those who learn the identities through general access to classified information are subject to a term not greater than ten 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).

[68] 50 U.S.C. § 3121.

[69] *Id.* § 3121(c).

information identifies a covert agent whose identity the United States is taking affirmative measures to conceal.[70] To date, there has been only one case interpreting the statute,[71] and only two convictions pursuant to guilty pleas have resulted from the statute.[72]

Section 1924 of Title 18 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.[73] The provision imposes a fine or a prison term of up to five years, or both, 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 to retain the materials at an unauthorized location.[74]

Section 952 of Title 18 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, imprisonment for up to ten 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,"[75] but not, apparently, for materials obtained during transmission from U.S. diplomatic missions abroad to the State Department or vice versa.[76] The 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. § 1924, which also applies only to U.S. government employees.[77]

Section 783 of Title 50 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.[78] It is also unlawful for the representative or agent of the foreign government to receive classified information.[79] Violation of either of these provisions is punishable by a fine of up to $10,000 or imprisonment for not more than ten years.[80] Violators are thereafter prohibited from holding federal public office.[81] 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.[82]

---

[70] *Id.* § 3121(a)–(c).

[71] United States v. Kiriakou, 2012 WL 3263854, at *4 (E.D. Va. Aug. 8, 2012) (rejecting the contention that "the statute was unconstitutionally vague because the statute does not define the 'affirmative measures' that the Government must take to conceal a covert agent's identity to trigger application of the statute").

[72] *See* Richard B. Schmitt, *Rare Statute Figures in Rove Case*, L.A. TIMES (July 15, 2005), https://www.latimes.com/archives/la-xpm-2005-jul-15-na-rove15-story.html (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 (Oct. 23, 2012), https://www.nytimes.com/2012/10/24/us/former-cia-officer-pleads-guilty-in-leak-case.html. (John Kiriakou pled guilty to disclosing a colleague's name to a journalist.)

[73] 18 U.S.C. § 1924.

[74] *Id.*

[75] *Id.* § 952.

[76] *Id.* Such transmissions may still be covered by the prohibition if the material was, or purports to have been, prepared using an official diplomatic code. It is unclear whether messages that are encrypted for transmission are covered.

[77] *See id.* § 1924(a).

[78] 50 U.S.C. § 783(a).

[79] *Id.* § 783(b).

[80] *Id.* § 783(c).

[81] *Id.*

[82] *Id.* § 783(e).

The Atomic Energy Act of 1954, 42 U.S.C. § 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,[83] or who has "reason to believe such data" would have that effect.[84]

Finally, 18 U.S.C. § 2381 creates a criminal prohibition on treason punishable by death, imprisonment, or fine.[85] The statute applies when a person "owing allegiance to the United States" levies war against the country or gives its enemies "aid and comfort"[86]—a term which has been interpreted to include transmitting information to foreign agents.[87]

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.[88] 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.[89] 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).[90]

Mens Rea and the Espionage Act

Sections 793(a)–(c) and 794 of Title 18, *U.S. Code* (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.... "[91] In *Gorin*, the Supreme Court concluded that this provision requires the defendant to have acted in bad faith against the United States.[92]

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

[83] 42 U.S.C. § 2274.

[84] *Id.* § 2274(b).

[85] 18 U.S.C. § 2381. The treason statute is predicated on Article III, Section 3 of the Constitution, which states: "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." U.S. CONST. art. III, § 3.

[86] 18 U.S.C. § 2381.

[87] *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.").

[88] For more background on mens rea requirements in federal criminal law, see CRS Report R46836, *Mens Rea: An Overview of State-of-Mind Requirements for Federal Criminal Offenses*, by Michael A. Foster. For scholarly treatment of the complex intent requirements in applicable statutes, see Papandrea, *supra* note 43.

[89] *Mens rea*, 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.").

[90] *See* Model Penal Code § 2.02(2) (defining "Kinds of Culpability").

[91] 18 U.S.C. §§ 793(a)–(c); 794(a).

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

information *could be* used to injure the United States or to advantage a foreign nation.[93] The Supreme Court has described the "willful" standard in some contexts as requiring that the accused was aware that his or her conduct violated the law.[94] 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*.[95] 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.[96]

Section 793(f) of Title 18 is unique in that it punishes the loss or removal of national defense information resulting from "gross negligence."[97] This standard has been described in other contexts as "the failure to exercise even a slight degree of care."[98] Prosecutions under the gross negligence provision of 18 U.S.C. § 793(f) appear to be rare,[99] 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.[100]

---

[93] 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).

[94] *See* Bryan v. United States, 524 U.S. 184, 192 (1998); Ratzlaf v. United States, 510 U.S. 135, 141 (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), *cert. denied*, 454 U.S. 1144 (1982).

[95] 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* N.Y. Times Co. 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. See, *e.g.* 18 U.S.C. § 793(f).

[96] *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).

[97] 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, ... 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.").

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

[99] 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 twenty-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. Eric Lichtblau, *F.B.I. Agent Pleads Guilty In Deal in Chinese Spy Case*, N.Y. TIMES (May 13, 2004), https://www.nytimes.com/2004/05/13/us/fbi-agent-pleads-guilty-in-deal-in-chinese-spy-case.html.

[100] *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 (continued...)

Other Mens Rea Requirements

Apart from the Espionage Act, 18 U.S.C. § 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 in some contexts requires the defendant to have been aware that his or her conduct was wrongful.[101] Other prohibitions on the disclosure of protected information incorporate the knowing standard either in conjunction with other mens rea requirements[102] or standing alone.[103]

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 ten years imprisonment and a $50,000 fine.[104] Separate provisions apply when government employees or contractors or military officials disclose restricted information identified in the Atomic Energy Act.[105]

Although some modern statutes create what are known as strict liability offenses that require no mens rea at all,[106] 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."[107] Policymakers are faced with the task of balancing these interests within the framework created by the Constitution.

---

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/.

[101] *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"))).

[102] *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).

[103] *See id.* § 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).

[104] 42 U.S.C. § 2274.

[105] *See id.* § 2277.

[106] *Liability*, BLACK'S LAW DICTIONARY (10th ed. 2014).

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

The First Amendment to the U.S. Constitution provides that "Congress shall make no law ... abridging the freedom of speech, or of the press."[108] 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."[109] The Supreme Court has described protection of the nation's security from external threat as a classic example of a compelling government interest.[110] 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.[111] Speech likely to incite immediate violence, for example, may be suppressed.[112] Speech that would give military advantage to a foreign enemy is also susceptible to government regulation.[113]

Where First Amendment rights are implicated, it is the government's burden to show that its interest is sufficiently compelling to justify enforcement.[114] 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.[115] Actual damage need not be proved, but potential damage must be more than merely speculative and incidental.[116] On the other hand, the Supreme Court has stated that "state action to punish the publication of truthful information seldom can satisfy constitutional standards."[117] The Court further described the constitutional purpose behind the guarantee of press freedom as the protection of "the free discussion of governmental affairs."[118]

---

[108] *Id.*, amend. I. For an analysis of exceptions to the First Amendment, see CRS In Focus IF11072, *The First Amendment: Categories of Speech*, by Victoria L. Killion.

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

[110] *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)).

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

[112] Brandenburg v. Ohio, 395 U.S. 444, 447 (1969).

[113] 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.").

[114] United States v. Playboy Ent. Grp., Inc., 529 U.S. 803, 813 (2000) ("If a statute regulates speech based on its content, it must be narrowly tailored to promote a compelling Government interest.") (citing Sable Communications of Cal., Inc. v. FCC, 492 U.S. 115, 126 (1989)).

[115] *National security* is defined as national defense and foreign relations. *See* Exec. Order No. 13,526, § 6.1(cc), 3 C.F.R. § 13526 (2010).

[116] *See, e.g.*, N.Y. 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)).

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

[118] 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 (continued...)

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,[119] 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."[120] 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.[121] Typically, courts have been unwilling to review executive branch decisions related to national security, or have relied on a strong presumption that the material at issue is potentially damaging.[122] 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.[123]

The courts seem 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

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* Cong. Rsch. Serv., *Overview of Freedom of the Press*, CONSTITUTION ANNOTATED, https://constitution.congress.gov/browse/essay/amdt1-9-1/ALDE_00000395/ (last visited May 1, 2023).

[119] Exec. Order No. 13,526, § 1.2, 3 C.F.R. § 13526 (2010), ("Classified National Security Information"). Section 1.2 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. *Id.*

[120] 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).

[121] *See, e.g.*, United States v. Abu-Jihaad, 600 F. Supp. 2d 362, 385–86 (D. Conn. 2009) (holding that 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).

[122] *See, e.g.*, Haig v. Agee, 453 U.S. 280, 292 (1981) ("Matters intimately related to foreign policy and national security are rarely proper subjects for judicial intervention.").

[123] *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).

respect to federal employees.[124] Although courts have not held that government classification of material is sufficient to show that its release is damaging to national security,[125] 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.[126]

Select Prosecutions of Leaks and Disclosures

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.[127] As cases described below demonstrate, criminal defendants have been successfully prosecuted even when claiming to have an altruistic desire to expose potentially important information regarding government activities to the press, public policy advocacy organizations, and others.[128] 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,[129] 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 select criminal prosecutions, both successful and unsuccessful, for leaks and other unauthorized disclosures to the press, policy advocacy groups, or others.[130]

---

[124] *See* Snepp v. United States, 444 U.S. 507, 510 (1980) (stating that "this Court's cases make clear that—even in the absence of an express agreement—the CIA could have acted to protect substantial government interests by imposing reasonable restrictions on employee activities that in other contexts might be protected by the First Amendment."); *Morison*, 844 F.2d at 1076 (observing that the espionage statutes "are expressions of an important and vital governmental interest."); *id.* at 1073 (finding that, due to "defendant's own expertise in the field of governmental secrecy and intelligence operations, the language of the statutes, 'relating to the national security' was not unconstitutionally vague as applied to this defendant."); United States v. Marchetti, 466 F.2d 1309, 1313 (4th Cir. 1972) (agreeing that "the First Amendment limits the extent to which the United States, contractually or otherwise, may impose secrecy requirements upon its employees and enforce them with a system of prior censorship" but that "we are here concerned with secret information touching upon the national defense and the conduct of foreign affairs"), *cert. denied*, 409 U.S. 1063 (1972).

[125] *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.)

[126] *See* United States v. Dedeyan, 584 F.2d 36, 39 (4th Cir. 1978).

[127] *See, e.g.*, United States v. Morison, 844 F.2d 1057, 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).

[128] *See, e.g.*, *infra* §§ "Samuel Loring Morison and *Jane's Defence Weekly*; Shamai Leibowitz, Leaked Transcripts of Calls with the Israeli Embassy; Jeffrey Sterling, CIA Disclosures to *New York Times* Reporter James Risen; Private Manning and WikiLeaks; Reality Winner, Leaked Document to the Intercept."

[129] 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." 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, National Security Agency Disclosures to the *Baltimore Sun*."

[130] For an analysis of incidents that include 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). For a list of other prosecutions for unlawful retention or other misuse of classified information, see Jeff Seldin, *FBI, Justice Department Routinely Prosecute Misuse of Classified Documents*, VOA NEWS (Aug. 9, 2022), https://www.voanews.com/a/fbi-justice-department-routinely-prosecute-misuse-of-classified-documents/6694887.html.

The Criminal Prosecution for the Pentagon Papers Leak

One highly publicized 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 on the role of the United States in the Vietnam War, which came to be known as the Pentagon Papers.[131] Ellsberg claimed he orchestrated the leak in an effort to influence public opinion and help bring about an end to the Vietnam War.[132] In addition to filing a civil action to block the *New York Times* and *Washington Post* from publishing the Pentagon Papers, discussed below,[133] the government brought criminal charges against Ellsberg and Russo for violations of 18 U.S.C. § 793, conversion of government property, and conspiracy.[134] 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.[135]

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 court opinion arising from his prosecution, *United States v. Morison*, produced an important delineation of the requirements for conviction under the Espionage Act.[136] 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.[137] 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.[138] 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[139]—was not

[131] 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.

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

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

[134] 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).

[135] For further background on the history of the case and the court's decision to declare a mistrial, see Melville B. 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), https://archive.nytimes.com/www.nytimes.com/learning/general/onthisday/big/0511.html.

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

[137] *Morison*, 844 F.2d at 1061–63.

[138] *Id.* at 1080.

[139] *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), https://harpers.org/archive/1989/09/the-quiet-coup/.

found to negate the element of intent.[140] The Fourth Circuit also rejected Morison's argument that the First Amendment protects unauthorized disclosures to the press.[141]

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 or the courts that he lacked culpability. The Department of Justice (DOJ) did, however, come under some criticism on the basis that such prosecutions are so rare as to amount to a selective prosecution in Morrison's 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.[142] On leaving office, President Clinton pardoned Morison.[143]

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), a lobbying group focused on U.S.-Israel relations.[144] 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,[145] 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.[146] 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.[147]

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

[140] *Morison*, 844 F. 2d at 1073–74.

[141] *See id.* at 1069–70 ("[I]t seems beyond controversy that a recreant intelligence department employee who had abstracted from the government files secret intelligence information and had wilfully transmitted or given it to one 'not entitled to receive it' as did the defendant in this case, is not entitled to invoke the First Amendment as a shield to immunize his act of thievery. To permit the thief thus to misuse the Amendment would be to prostitute the salutary purposes of the First Amendment.").

[142] *See* Jack Nelson, *U.S. Government Secrecy and the Current Crackdown on Leaks* 8 (The Joan Shorenstein Ctr. on the Press, Pol. and Pub. Pol'y, Working Paper Series 2003-1, 2002), https://shorensteincenter.org/wp-content/uploads/2012/03/2003_01_nelson.pdf; Ben A. Franklin, *Morison Receives 2-Year Jail Term*, N.Y. TIMES (Dec. 5, 1985), https://www.nytimes.com/1985/12/05/us/morison-receives-2-year-jail-term.html (noting criticism of the prosecution as a threat to freedom of the press).

[143] Clinton's Pardons, January 2001, https://www.justice.gov/archives/opa/president-clintons-pardons-january-2001 (last updated Oct. 5, 2022). 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 Daniel Patrick Moynihan, U.S. Sen., to President Bill Clinton (Sep. 29, 1998), http://www.fas.org/sgp/news/2001/04/moynihan.html.

[144] For further detail on the AIPAC disclosure, see Lee, *supra* note 16, at 167–75.

[145] See *id.* at 167.

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

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

FBI.[148] The government accused Leibowitz of disclosing classified information to a blogger in violation of 18 U.S.C. § 798, but it never publicly identified the exact information disclosed or the identity of the blogger.[149] Media outlets reported that Leibowitz disclosed transcripts of conversations caught on FBI wiretaps of the Israeli Embassy in Washington, D.C.[150] Leibowitz reportedly claimed that his intention was to expose official misconduct, not damage national security,[151] but he ultimately pled guilty and was sentenced to 20 months in prison.[152]

Thomas Drake, National Security Agency 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,[153] on ten felony charges for providing classified information regarding perceived mismanagement of NSA programs to the *Baltimore Sun*.[154] Drake's original indictment included five counts under the Espionage Act,[155] but the prosecution's case suffered setbacks after it was revealed that much of the information at issue was either not classified or had been publicly discussed by other government officials,[156] 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.[157] Drake eventually pled guilty to a single misdemeanor for exceeding his authorized use of an NSA computer.[158] Prior to issuing its sentence of one year probation and 240 hours of community service, the court reportedly called the government's treatment of Drake in the case "unconscionable," and it declined to impose a fine.[159]

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.[160] Sterling disclosed information

---

[148] Former FBI Contract Linguist Pleads Guilty to Leaking Classified Information to Blogger (Dec. 17, 2009), https://www.justice.gov/opa/pr/former-fbi-contract-linguist-pleads-guilty-leaking-classified-information-blogger.

[149] *See* Indictment of Shamai Kedem Leibowitz at 1, United States v. Leibowitz, No. AW09CR0632 (D. Md. Dec. 4, 2009), 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.

[150] *Id.*

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

[152] *Id.*; Vladeck, *Prosecuting Leaks*, *supra* note 134, at 31.

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

[154] Indictment of Thomas Drake, United States v. Drake, No. 1:10-cr-00181 (D. Md. Apr. 14, 2010), https://assets.documentcloud.org/documents/323707/drake-indictment.pdf.

[155] *Id.*

[156] *See* Downie & Rafsky, *supra* note 149.

[157] Motion to Dismiss the Indictment at the time of Sentencing, United States v. Drake, No. 1:10-cr-00181 (D. Md. June 10, 2011), http://www.fas.org/sgp/jud/drake/061011-dismiss.pdf.

[158] *See* Downie & Rafsky, *supra* note 149.

[159] *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.

[160] *See* United States v. Sterling, 724 F.3d 482, 488 (4th Cir. 2013), *reh'g en banc denied*, 732 F.3d 292, *cert denied*, (continued...)

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.[161] 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.[162] He was sentenced to forty-two months in prison.[163]

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.[164] Kim faced one count of violating the Espionage Act and one count of making false statements to the FBI.[165] 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,[166] Kim pled guilty to a single count of disclosing national defense information to a person not authorized to receive it in violation of 18 U.S.C. § 793(d).[167] He was sentenced to thirteen months in prison.[168]

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 a government classified system.[169] 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

572 U.S. 1149 (2014); *In re* Grand Jury Subpoena to Risen at 1–3, No. 1:10CR485, 2010 U.S. Dist. LEXIS 143340 (E.D. Va. Nov. 30, 2010); Indictment of Jeffrey Sterling, United States v. Sterling, 818 F. Supp. 2d 945 (E.D. Va. 2011) (No. 1:10CR485), https://assets.documentcloud.org/documents/323711/sterling-indictment.pdf.

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

[162] *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.

[163] *See* sources cited *supra* note 162.

[164] *See* United States v. 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.

[165] *Kim*, 808 F. Supp. 2d at 47.

[166] *Id.*

[167] 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 Ronald C. Machen Jr., U.S. Att'y, U.S. Dep't of Justice, to Counsel of Stephen Jim-Woo Kim (Feb. 2, 2014), https://fas.org/sgp/jud/kim/plea.pdf.

[168] U.S. Attorney's Office, District of Columbia, *Former Federal Contract Employee Sentenced to 13 Months in Prison for Disclosing National Defense Information* (Apr. 2, 2014), https://www.justice.gov/usao-dc/pr/former-federal-contract-employee-sentenced-13-months-prison-disclosing-national-defense; Marimow, *supra* note 164.

[169] *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).

capital punishment or life imprisonment[170]—and violating the Espionage Act as applied through Article 134 of the UCMJ.[171]

Manning pled guilty to ten charges, including some Espionage Act counts, but prosecutors pursued the remaining charges without seeking the death penalty.[172] In 2013, Manning was convicted by court-martial of all charges except aiding the enemy, and was sentenced to thirty-five years of imprisonment, reduction in rank, forfeiture of pay, and a dishonorable discharge.[173] On January 17, 2017, President Obama commuted Manning's sentence, which expired in May 2017.[174] The United States has also brought charges against Julian Assange for his role in connection with Private Manning's disclosures, discussed below.[175]

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.[176] 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[177] for providing the name of a covert CIA operative to a reporter.[178] While Kirkaou argued that he had been singled out for prosecution because of his earlier public criticism of the CIA,[179] he pled guilty to violating the Intelligence Identities Protection Act.[180] The remaining charges were dropped as part of his plea agreement,

[170] 10 U.S.C. § 904.

[171] *Id.* § 934. *See also* Ed Pilkington, *Bradley Manning May Face Death Penalty*, GUARDIAN (Mar. 2, 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).

[172] *See* Bakken, *supra* note 169; 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.

[173] *See* Andrew Aylward, *Manning Acquitted of Aiding the Enemy*, WALL. ST. J. (July 30, 2013), https://www.wsj.com/articles/SB10001424127887323854904578637681374754140; Sarah Childress, *Bradley Manning Sentenced to 35 Years for Wikileaks*, PBS FRONTLINE (Aug. 21, 2013), https://www.pbs.org/wgbh/frontline/article/bradley-manning-sentenced-to-35-years-for-wikileaks/.

[174] Press Release, 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.

[175] *See infra* "The Julian Assange Charges."

[176] *See* Indictment of John C. Kiriakou, United States v. Kiriakou, No. 1:12cr127 (LMB) (E.D. Va. Apr. 5, 2012), https://sgp.fas.org/jud/kiriakou/indict.pdf. *See also* Vladeck, *supra* note 134, at 33.

[177] 50 U.S.C. § 3121.

[178] Press Release, Dep't of Justice, Office of Public Affairs, 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.

[179] *See* Associated Press, *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.

[180] Press Release, 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.

and he was sentenced to thirty months in prison.[181] This case is reported to have been the first conviction under Intelligence Identities Protection Act in twenty-seven years.[182]

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. § 2071(a)[183] for providing certain classified information to the Hoover Institution,[184] a public policy think tank at Stanford University. Hitselberger, who claimed that his case was "overcharged,"[185] entered into a plea agreement in which all Espionage Act charges were dropped. He pled guilty to a single misdemeanor count of unlawful removal of classified material under 18 U.S.C. § 1924[186] for attempting to take certain classified materials outside of a secure work area.[187] He was sentenced to time served.[188]

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.[189] 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).[190] 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.[191] Sachtleben

---

[181] Dep't of Justice, U.S. Attorney's Office, *supra* note 180; Charlie Savage, *Former C.I.A. Operative Pleads Guilty in Leak of Colleague's Name*, N.Y. TIMES (Oct. 23, 2012), https://www.nytimes.com/2012/10/24/us/former-cia-officer-pleads-guilty-in-leak-case.html.

[182] 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.

[183] 18 U.S.C. § 2071(a).

[184] *See* Superseding Indictment, United States v. Hitselberger, No. 12-231 (D.D.C., filed Feb. 28, 2013), https://sgp.fas.org/jud/hitsel/indict-sup.pdf; Vladeck, *supra* note 134, 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.

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

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

[187] *See* Judgment, United States v. Hitselberger, No. 12-231 (D.D.C. filed July 18, 2014), https://sgp.fas.org/jud/hitsel/judgment.pdf; Superseding Information, United States v. Hitselberger, No. 12-231 (D.D.C. filed Apr. 25, 2014), https://sgp.fas.org/jud/hitsel/info-sup.pdf; 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.

[188] *See* Judgment, *supra* note 187.

[189] Statement of Offense, United States v. Sachtleben, No. 1:13-cr-0200 (S.D. In. filed Sep. 23, 2014), https://www.justice.gov/iso/opa/resources/764201392315452761880 2.pdf.

[190] *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 Bomb 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/.

[191] *See* Charlie Savage and Leslie Kaufman, *Phone Records of Journalists Seized by U.S.*, N.Y. TIMES (May 1, 2013,), (continued...)

ultimately pled guilty to two counts of violating the Espionage Act and was sentenced to forty-three months' imprisonment.[192]

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 to the *Guardian* (UK) and the *Washington Post*.[193] Snowden permitted the newspapers to publish his name, but fled to Hong Kong before he could be taken into custody. A still-pending criminal complaint charges Snowden with violating 18 U.S.C. §§ 793(d) and 798(a)(3) and theft of government property under 18 U.S.C. § 641.[194] Russia granted Snowden citizenship in December 2022, making it impossible under the Russian Federation's constitution to extradite him to the United States.[195]

General David Petraeus, Unauthorized Disclosure to Biographer

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. § 1924 in March 2015.[196] Petraeus was accused of disclosing classified information to an Army Reserve officer who was writing his biography and with whom Petraeus admitted to having a romantic relationship.[197] 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.[198] Petraeus pled guilty to the misdemeanor charge, and prosecutors

https://www.nytimes.com/2013/05/14/us/phone-records-of-journalists-of-the-associated-press-seized-by-us.html. Sari Horwitz & Carol D. Leonnig, *Holder is Back in the Crossfire After Justice Dept. Obtains AP Phone Records*, WASH. POST (May 14, 2013), https://www.washingtonpost.com/world/national-security/attorney-general-eric-holder-back-in-crossfire-after-justice-dept-obtains-ap-phone-records/2013/05/14/a045a01e-bcab-11e2-89c9-3be8095fe767_story.html.

[192] *See* Press Release, 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 into a plea agreement and pled guilty to child pornography-related offenses uncovered in an unrelated investigation. *Id.*

[193] *See* Devlin Barrett, *Snowden on the Run*, WALL ST. J. (June 24, 2013), https://www.wsj.com/articles/SB10001424127887323683504578562852310273818; Shaun Waterman, *NSA Leaker Ed Snowden Used Banned Thumb-drive, Exceeded Access*, WASH. TIMES (June 14, 2013), https://www.washingtontimes.com/news/2013/jun/14/nsa-leaker-ed-snowden-used-banned-thumb-drive-exce/.

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

[195] Andrew Roth, *Edward Snowden Gets Russian Passport After Swearing Oath of Allegiance*, GUARDIAN (Dec. 2, 2022), https://www.theguardian.com/us-news/2022/dec/02/edward-snowden-gets-russian-passport-after-swearing-oath-of-allegiance.

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

[197] *See* Jonathan Allen, Josh Gerstein, & Jennifer Epstein, *Citing Affair, Petraeus Resigns at CIA*, POLITICO (Nov. 11, 2012), https://www.politico.com/story/2012/11/gen-david-petraeus-resigns-08364; Michael S. Schmidt and Matt Apuzzo, *F.B.I. and Justice Dept. Said to Seek Charges for Petraeus*, N.Y. TIMES (Jan. 9, 2015), https://www.nytimes.com/2015/01/10/us/politics/prosecutors-said-to-recommend-charges-against-former-gen-david-petraeus.html.

[198] *See, e.g.*, sources cited *supra* note 197; *Petraeus Sentenced to 2 Years Probation for Military Leak*, FOXNEWS (Dec.
(continued...)

recommended a $40,000 fine as part of a plea agreement,[199] but the court imposed the maximum $100,000 fine based on what it deemed to be the serious nature of the crime.[200]

Reality Winner, Leaked Document to the Intercept

Reality Winner, an NSA contractor, was charged under the Espionage Act for providing the news website the Intercept a top-secret report revealing Russian efforts to hack voting machines during the 2016 election.[201] She pled guilty in 2018 to one count of unlawful retention and transmission of national defense information in violation of 18 U.S.C. § 793(e) and was sentenced to sixty-three months in prison and three years of supervised release.[202] She was released to a halfway house in June 2021 for good behavior[203] and subsequently released to her parents' home.[204]

Joshua Schulte, Disclosure of CIA Hacking Tools to WikiLeaks

Joshua Adam Schulte, a former CIA software engineer, was prosecuted in connection with the "Vault 7" leak of details regarding CIA tools and techniques for penetrating foreign computer and communications networks.[205] He was charged with unauthorized disclosure of national defense information, theft of government property, unauthorized access of a government computer, and transmission of harmful computer programs and code.[206] WikiLeaks began publishing the files in 2017, claiming that the entire archive contained several hundred million lines of computer

20, 2015), http://www.foxnews.com/politics/2015/04/23/petraeus-sentenced-to-2-years-probation-for-military-leak.html; Adam Goldman, *Petraeus Pleads Guilty to Mishandling Classified Material, Will Face Probation*, WASH. POST. (Apr. 22, 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.

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

[200] *See* Ken Otterbourg & Andrew Grossman, *Gen. David Petraeus Avoids Jail Time, to Pay $100,000 Fine: Former CIA Director Pleased Guilty in Agreement with Justice Department*, WALL ST. J. (Apr. 23, 2015), https://www.wsj.com/articles/david-petraeus-sentenced-to-two-years-probation-1429816999.

[201] Press Release, Dep't of Justice, Office of Public Affairs, Federal Government Contractor in Georgia Charged With Removing and Mailing Classified Materials to a News Outlet (Jun. 5, 2017), https://www.justice.gov/opa/pr/federal-government-contractor-georgia-charged-removing-and-mailing-classified-materials-news; Criminal Complaint, United States v. Winner, No. 1:17-mj-00024 (S.D. Ga. June 5, 2017), https://www.justice.gov/opa/press-release/file/971336/download; Affidavit in Support of Application for Arrest Warrant, United States v. Winner, No. 1:17-mj-00024 (S.D. Ga. June 5, 2017), https://www.justice.gov/opa/press-release/file/971331/download; Amanda Holpuch, *Reality Winner: NSA Contractor Jailed for Five Years over Classified Report Leak*, GUARDIAN (Aug. 23, 2018), https://www.theguardian.com/us-news/2018/aug/23/reality-winner-sentence-classified-report-leak.

[202] Press Release, Dep't of Justice, Office of Public Affairs, Federal Government Contractor Sentenced for Removing and Transmitting Classified Materials to a News Outlet (Aug. 23, 2018), https://www.justice.gov/opa/pr/federal-government-contractor-sentenced-removing-and-transmitting-classified-materials-news.

[203] Julian E. Barnes, *Reality Winner, Who Leaked Government Secrets, is Released from Prison*, N.Y. TIMES (Jun. 14, 2021), https://www.nytimes.com/2021/06/14/us/politics/reality-winner-is-released.html.

[204] *See Reality Winner Says She Leaked File on Russia Election Hacking because 'Public was Being Lied To'*, GUARDIAN (July. 25, 2022), https://www.theguardian.com/us-news/2022/jul/25/reality-winner-leaked-file-on-russia-election-hacking-because-public-was-being-lied-to.

[205] *See* Superseding Indictment, United States. v. Schulte, Case No. S1 17 Cr. 548, (S.D. N.Y. 2018), https://www.justice.gov/usao-sdny/press-release/file/1072871/download [Schulte Indictment].

[206] *See* Schulte Indictment, *supra* note 205. Press Release, U.S. Attorney's Office, Southern District of New York, Joshua Adam Schulte Charged with the Unauthorized Disclosure of Classified Information and Other Offenses Relating to the Theft of Classified Material from the Central Intelligence Agency (Jun. 18. 2018), https://www.justice.gov/usao-sdny/pr/joshua-adam-schulte-charged-unauthorized-disclosure-classified-information-and-other.

code.[207] Schulte was convicted in 2022 on nine counts related to the theft and transmission of the material and lying to the FBI.[208] Schulte has not yet been sentenced but could face eighty years in prison.[209]

Jack Teixeira, Charged with Posting Classified Documents in Online Chat Room

Massachusetts Air National Guardsman Jack Teixeira was charged with violating 18 U.S.C. §§ 793(b) and (d) and 1924 for posting transcriptions and images of dozens of classified documents to an online social media site beginning in December 2022.[210] The twenty-one-year-old airman had access to the documents due to his role as an information technology specialist in the 102nd Intelligence Wing, headquartered on Otis Air National Guard Base in Eastern Massachusetts.[211] The disclosed materials described intelligence concerning the war in Ukraine and other matters involving U.S. adversaries as well as allies.[212] The government has asked a magistrate judge to deny his request to be released on bail.[213]

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,[214] the government has never prosecuted a traditional news organization for its *receipt* of classified or other protected information.[215] The plain terms of the Espionage Act, however, do not focus solely on the initial disclosure of national defense information.[216] While

[207] Shane Harris, *Wikileaks Dumps Trove of Purported CIA Hacking Tools*, WALL ST. J. (Mar. 7, 2017), https://www.wsj.com/articles/wikileaks-posts-thousands-of-purported-cia-cyberhacking-documents-1488905823.

[208] Danielle Wallace, *Ex-CIA Engineer Convicted of Biggest Theft of Secret Information in Agency's History*, FOX NEWS (July 14, 2022), https://www.foxnews.com/us/ex-cia-engineer-convicted-biggest-theft-secret-information-agencys-history. The conviction was for four counts of espionage in violation of 18 U.S.C. §§ 793(b) and (e), four counts of computer hacking in violation of 18 U.S.C. § 1030(a), and one count of obstructing justice in violation of 18 U.S.C. § 1503. The Government's Memorandum of Law in Opposition to the Defendant's *Pro Se* Motions for a Judgment of Acquittal or New Trial at 6, United States v. Schulte, No. 1:17-cr-00548 (S.D.N.Y. filed Mar. 16, 2023), https://ia601400.us.archive.org/13/items/gov.uscourts.nysd.480183/gov.uscourts.nysd.480183.1021.0.pdf.

[209] *See* U.S. Attorney's Office, Southern District of New York, *supra* note 206.

[210] Criminal Complaint and Affidavit in Support of an Application for a Criminal Complaint and Arrest Warrant, United States v. Teixeira, No. 23-4293-DHH (Apr. 14, 2023, D. Mass.), *available at* https://www.documentcloud.org/documents/23777290-case-1-23-mj-04293-dhh.

[211] John Ismay & Jenna Russell, *Massachusetts Air National Guard's Intelligence Mission in the Spotlight*, N.Y. TIMES (Apr. 13, 2023), https://www.nytimes.com/2023/04/13/us/leaked-documents-massachusetts-air-national-guard.html.

[212] Daniel Victor, *Leaked Documents Revealed Secret U.S. Intelligence, What Did They Say?*, N.Y. TIMES (Apr. 13, 2023), https://www.nytimes.com/live/2023/04/13/us/documents-leak-pentagon?smid=url-share#leaked-documents-revealed-secret-us-intelligence-what-did-they-say.

[213] Shelley Murphy, Air National Guardsman Accused of Leaking Classified Military Documents Due in Court for Second Hearing on Possible Bail, BOSTON GLOBE (May 8, 2023), Air National Guardsman accused of leaking classified military documents due in court for second hearing on possible bail (msn.com).

[214] *See infra* § "Select Prosecutions of Leaks and Disclosures."

[215] Papandrea, *supra* note 43, at 1389. *See also House Judiciary WikiLeaks Hearing*, *supra* note 2, at 39–40, 43 (statement of Kenneth L. Wainstein, former Assistant Attorney General, Partner, O'Melveny & Myers, LLP).

[216] *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 (continued...)

there is some authority for interpreting portions of the Espionage Act as to exclude "publication" of material from the criminal provisions,[217] 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.[218] In two prosecutions, one of which was dropped, the United States has pursued criminal charges against individuals other than the initial leaker for the individuals' roles in soliciting and facilitating the leaks.[219]

The role of the press in leak prosecutions became the subject of frequent discussion among legal and media commentators following a series of cases in which the government sought to gather evidence from the media about their sources through secret subpoenas that were not made known to their targets.[220] The following section discusses these 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.

The Civil Litigation in the *Pentagon Papers* Case

The primary legal precedent governing the potential prosecution of the press for publishing leaked information is the Supreme Court's *Pentagon Papers* decision.[221] 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.[222] The consolidated case quickly reached the Supreme Court,[223] 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.[224] 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 majority of Supreme Court Justices recognized a high level of First Amendment protection afforded to the

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").

[217] *See* N.Y. 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).

[218] *See, e.g.*, *House Judiciary WikiLeaks Hearing*, *supra* note 2, 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 12, at 231–32.

[219] *See infra* §§ "Criminal Prosecution of AIPAC Lobbyists in *United States v. Rosen*; "The Julian Assange Charges."

[220] *See, e.g.*, Vladeck, *supra* note 12, at 231–32; Lee, *supra* note 16, 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.

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

[222] *See id.*

[223] DOJ filed its first complaint against the New York Times on June 14, 1971, JAKE KOBRICK, THE PENTAGON PAPERS IN THE FEDERAL COURTS 2 (2019), 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.

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

press in the *Pentagon Papers* case.[225] The Court's decision to deny the injunction may inform decisions involving criminal prosecutions of the press or other media organizations.[226]

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 opinions 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.[227] Still, in 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.[228]

The publication of truthful information that is lawfully acquired enjoys considerable First Amendment protection.[229] 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."[230] (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.[231] However, what constitutes "routine newsgathering" has not been further elucidated. In a 2001 case, *Bartnicki v. Vopper*, the Court cited the *Pentagon Papers* case holding 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.[232] The holding suggests that recipients of unlawfully disclosed information cannot be considered to have

[225] *See id.* at 717 (Black, J. with Douglas, J., concurring) ("Both the history and language of the First Amendment support the view that the press must be left free to publish news, whatever the source, without censorship, injunctions, or prior restraints."); *id.* at 720 (Douglas, J. with Black, J., concurring) (interpreting the First Amendment to leave "no room for governmental restraint on the press"); *id.* at 725 (Brennan, J., concurring) ("[T]he First Amendment stands as an absolute bar to the imposition of judicial restraints in circumstances of the kind presented by these cases."); *id.* at 728 ((Stewart, J. with White, J., concurring) ("[W]ithout an informed and free press there cannot be an enlightened people."); *id*. at 730–31, (White, J. with Stewart, J., concurring) (emphasizing the "concededly extraordinary protection against prior restraints enjoyed by the press under our constitutional system").

[226] *See* Papandrea, *supra* note 43, 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 215, 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).

[227] *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 also* David Topol, Note, *United States v. Morison: A Threat to the First Amendment Right to Publish National 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).

[228] *See* 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.

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

[230] 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.

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

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

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.[233]

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

The first 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.[234] 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*.[235] 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.[236] Some observers argued that the prosecution effectively criminalized the exchange of information,[237] 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, which some national security journalists consider to be an ordinary part of their job.[238]

The government eventually dropped the charges, 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.[239] With respect to the intent requirement under the Espionage

[233] *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).

[234] *See infra* § "Lawrence Franklin and the AIPAC Disclosure."

[235] *See* 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 also* Jerry Markon, *U.S. Drops Case Against Ex-Lobbyists*, N.Y. TIMES (May 2, 2009), https://www.nytimes.com/2009/05/02/us/politics/02aipac.html (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 that 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 DOJ to drop the matter so as not to draw attention to the United States' intelligence capabilities. *See id.*; Geoffrey R. Stone, *Roy R. Ray Lecture: Freedom of the Press in Time of War*, 59 SMU L. REV. 1663, 1668 (2006); House Judiciary WikiLeaks Hearing, *supra* note 215, at 61 (statement of Gabriel Schoenfeld).

[236] *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").

[237] Editorial, *Time to Call It Quits: The Justice Department Should Drop its Misguided Prosecution of Two Former AIPAC Officials*, WASH. POST, March 11, 2009, at A14 (editorial urging Attorney General to drop charges).

[238] *See* Lee, *supra* note 16, 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 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.

[239] *See* Tabassum Zakaria, *U.S. to Drop Israel Lobbyist Case*, REUTERS (May 1, 2009),
(continued...)

Act, the judge interpreted the term *willfully* in connection with the phrase *reason to believe it 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."[240] 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.[241]

The Julian Assange Charges

The government's charges against Julian Assange are also relevant to whether a publisher of classified information is subject to the Espionage Act. Whereas Private Manning was prosecuted under the UCMJ before a court-martial, a grand jury empaneled in a Virginia federal court investigated civilian involvement in Manning's leaks.[242] In 2018, the grand jury indicted Julian Assange for conspiracy to commit computer intrusion under 18 U.S.C. §§ 371 and 1030 related to the Manning leaks.[243] Superseding indictments have added multiple Espionage Act charges.[244]

The United States alleges Assange solicited and assisted Private Manning and others in efforts to obtain unauthorized access to government and private computer networks and in disseminating national defense information gained through that unlawful access.[245] Assange was arrested in the United Kingdom in 2019 and is fighting extradition to the United States.[246] He has appealed his extradition at London's High Court and to the European Court of Human Rights.[247]

Some observers argue that the Assange prosecution chills freedom of the press by seeking to punish Assange for receiving and publishing newsworthy government secrets in a manner that is

---

https://www.reuters.com/article/us-security-pentagon/u-s-to-drop-israel-lobbyist-spy-case-idUKTRE54046320090501 (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, 1084 (4th Cir. 1988) (Wilkinson, J., concurring)).

[240] *Rosen*, 445 F. Supp. 2d at 626.

[241] *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).

[242] Press Release, Dep't of Justice, Office of the Press Secretary, WikiLeaks Founder Charged in Superseding Indictment, (Jun. 24, 2020), https://www.justice.gov/opa/pr/wikileaks-founder-charged-superseding-indictment. *See* Second Superseding Indictment, United States v. Assange, No. 1:18cr00111 (CMH), https://www.justice.gov/opa/press-release/file/1289641/download.

[243] Indictment of Julian Assange, United States v. Assange, No. 1:18cr00111 (CMH) (E.D. Va. Mar. 6, 2018) https://www.justice.gov/opa/press-release/file/1153486/download.

[244] Second Superseding Indictment, United States v. Assange, No. 1:18cr00111 (CMH), https://www.justice.gov/opa/press-release/file/1289641/download.

[245] *See id*.

[246] *See*, *e.g.*, Jamie Grierson and Ben Quinn, *Julian Assange's Extradition from UK to US Approved by Home Secretary*, GUARDIAN (Jun. 17, 2022), https://www.theguardian.com/media/2022/jun/17/julian-assange-extradition-to-us-approved-by-priti-patel.

[247] Michael Holden, *Julian Assange Appeals to European Court over U.S. Extradition*, REUTERS (Dec. 2, 2022), https://www.reuters.com/world/julian-assange-appeals-european-court-over-us-extradition-2022-12-02/.

similar to traditional national security journalism.[248] DOJ contends that this case differs from traditional journalism because, according to the indictment, Assange actively solicited and assisted in obtaining classified information and published that information in an unredacted form and in a manner that created "grave and imminent risk" to U.S. intelligence sources identified in the leaked documents.[249]

Gathering Evidence from the Press and Department of Justice Media Policies

On some occasions, legal disputes have arisen out of the government's efforts to obtain testimony or records from the members of the press as part of leak prosecutions. In the trial of former CIA officer Jeffrey Sterling,[250] the Obama Administration sought to compel *New York Times* reporter James Risen to testify regarding classified information that the prosecution believed Sterling had provided to Risen.[251] Following Risen's motion to quash the trial subpoena, the district court concluded that, under the First Amendment, there is a qualified reporter's privilege that may be invoked when a subpoena seeks information about confidential sources or is intended to harass the journalist.[252] The district court limited the scope of Risen's testimony such that he was not compelled to reveal his confidential source.[253] On appeal, the U.S. Court of Appeals for the Fourth Circuit reversed the ruling, holding that there is neither a First Amendment privilege nor a federal common-law privilege protecting journalists from being compelled to testify.[254] Despite prevailing on appeal, the government did not call Risen to testify at the jury trial.[255]

In the investigation of Donald Sachtleben over leaks of covert efforts to foil a bomb plot on a U.S.-bound airliner,[256] media outlets reported that DOJ was unable to identify the source of the leaks until it issued subpoenas to obtain the calling records for twenty telephone lines associated with AP bureaus and reporters.[257] The targets of the subpoenas at the AP were reportedly not notified that their information was being collected, prompting some members of the media to criticize the government's evidence-gathering methods.[258]

---

[248] *See, e.g.*, Gabe Rottman, *The Assange Indictment Seeks to Punish Pure Publication*, LAWFARE (May 24, 2019), https://www.lawfareblog.com/assange-indictment-seeks-punish-pure-publication.

[249] Press Release, Dep't of Justice, Remarks from the Briefing Announcing the Superseding Indictment of Julian Assange 1 (May 23, 2019), https://www.justice.gov/opa/press-release/file/1165636/download (prepared remarks by Assistant Attorney General for National Security John C. Demers).

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

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

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

[253] *Id.* at 960.

[254] *Sterling*, 724 F.3d at 504–05.

[255] *See* Brief of Defendant-Appellant Jeffrey Alexander Sterling 13, *Sterling*, 724 F.3d 482 (4th Cir. 2013) (No. 15-4297) (filed Feb. 22, 2016), https://sgp.fas.org/jud/sterling/022216-brief.pdf.

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

[257] *See* Charlie Savage, *Former F.B.I. Agent to Plead Guilty in Press Leak*, N.Y. TIMES (Sep. 23, 2013), https://www.nytimes.com/2013/09/24/us/fbi-ex-agent-pleads-guilty-in-leak-to-ap.html?searchResultPosition=1.

[258] *See, e.g.*, Milbank, *supra* note 220; Ravi Somaiya, *Head of the A.P. Criticizes Seizure of Phone Records*, N.Y. TIMES (May 19, 2013), https://www.nytimes.com/2013/05/20/business/media/head-of-the-ap-criticizes-seizure-of-phone-records.html. *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.

Similarly, the case of former State Department contractor Stephen Jin-Woo Kim's disclosures to Fox News correspondent James Rosen generated attention when media outlets reported that DOJ subpoenaed Rosen's emails without notice.[259] Some observers asserted that the affidavit supporting the subpoena suggested Rosen could be charged for violating the Espionage Act by receiving classified information from a confidential source, but Rosen was never charged with a crime.[260]

After these events, the Obama Administration convened a series of stakeholder meetings to evaluate DOJ's policies and practices for collecting evidence from the media.[261] DOJ issued a report on its revised policies in 2013 that, among other things, modified its notification procedures before gathering evidence from the press and stated that "members of the news media will not be subject to prosecution based solely on newsgathering activities."[262] In what DOJ described as its "most significant change," the revised policies required DOJ to provide notice to and negotiate with members of the media before seeking their records related to newsgathering activities unless the Attorney General determined that advance notice would pose a clear and substantial threat to the integrity of the investigation, risk grave harm to national security, or present an imminent risk of death or injury.[263] According to the report, the notice and negotiation requirements would apply "in all but the most exceptional cases."[264]

During the Trump Administration and the early months of the Biden Administration, some media outlets reported that government officials sought evidence from members of the press related to their confidential sources in ways that raised questions as to whether DOJ was complying with its news media policies.[265] In July 2021, Attorney General Merrick Garland announced that he had revised DOJ's media policy to state that DOJ would no longer use subpoenas or other compulsory legal process[266] to obtain information from "members of the news media acting within the scope

[259] See Application for a Search Warrant, Affidavit in Support of Application for a Search Warrant, and Search and Seizure Warrant 3, P 3, No. 10-291-M-01 (D. D.C. Nov. 7, 2011) [hereinafter, "Rosen Warrant Affidavit"]; Charlie Savage, *Ex-Contractor at State Dept. Pleads Guilty in Leak Case*, N.Y. TIMES (Feb. 8, 2014,). https://www.nytimes.com/2014/02/08/us/politics/ex-state-department-contractor-pleads-guilty-in-leak-case.html. *See also* Etzioni *supra* note 258, at 1143-44.

[260] *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 220; Editorial, *Justice Department Run Amok on Journalists' Sources*, S.F. CHRON. (May 22, 2013), http://www.sfchronicle.com/opinion/editorials/article/Justice-Department-run-amok-on-journalists-4540632.php. 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," 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." Rosen Warrant Affidavit, *supra* note 259, at 26-27.

[261] DEP'T OF JUSTICE, REPORT ON NEWS MEDIA POLICIES (July 12, 2013), https://www.justice.gov/sites/default/files/ag/legacy/2013/07/15/news-media.pdf [hereinafter, "2013 Media Policies Report"].

[262] *Id.* at 2. DOJ made additional revisions to media guidelines in 2015. *See* Policy Regarding Obtaining Information from, or Records of, Members of the News Media; and Regarding Questing, Arresting, or Charting Members of the News Media, 80 Fed. Reg. 2819 (Jan. 21, 2015) (codified at 28 C.F.R. pt. 50); Press Release, Dep't of Justice, Office of Public Affairs, Attorney General Holder Announces Update to Justice Department Media Guidelines (Jan. 14, 2015), https://www.justice.gov/opa/pr/attorney-general-holder-announces-updates-justice-department-media-guidelines.

[263] 2013 Media Policies Report, *supra* note 261, at 2.

[264] *Id.*

[265] For background on the post-2013 subpoenas and other compulsory legal process used to obtain evidence from members of the media, see Secrecy Orders Hearing, *see supra* note 2, at 6–49.

[266] Compulsory legal process includes "subpoenas, search warrants, court orders issued pursuant to 18 U.S.C. 2703(d)
(continued...)

of [their] newsgathering activities."[267] DOJ issued new regulations, 28 C.F.R. § 50.10, incorporating the revised policy in October 2022.[268]

The revised media policy includes certain limits and exceptions on its restrictions.[269] In particular, the prohibition on subpoenas and compulsory process does not apply when the member of the news media is not acting within the scope of *newsgathering*.[270] The regulations define *newsgathering* as the process of pursuing or obtaining information for purposes of producing content intended for public dissemination.[271] The regulations do not define *member of the news media*, but they do include a process for resolving close or novel questions about a person's media status and whether the person was engaged in newsgathering.[272] The regulations also do not apply when there are reasonable grounds to believe that the member of the media is an agent of a foreign power or a member or affiliate of a foreign terrorist organization or related terrorist entity or is engaged in certain terrorism-related activity.[273]

Considerations for Congress and Recent Legislative Proposals

Criminal prohibitions on leaks and other unauthorized disclosures of protected government information highlight the tension between the public's interest in government activity and the United States' interest in operating effectively and protecting national security.[274] Some observers describe the current laws protecting classified information as a patchwork of mostly outdated provisions that are vague and inconsistent[275] or assert that these laws may not cover all the information the government legitimately needs to protect.[276] Others argue that the laws fail to take sufficient consideration of the value of releasing to the public information that the government

and 3123, interception orders issued pursuant to 18 U.S.C. 2518, civil investigative demands, and mutual legal assistance treaty requests.... " 28 C.F.R. § 50.10(b)(2).

[267] Memorandum from the Office of the Att'y Gen. on Use of Compulsory Process to Obtain Information from, or Records of, Members of the News Media 1 (July 19, 2021), https://www.justice.gov/ag/page/file/1413001/download.

[268] Memorandum from the Office of the Att'y Gen. on New Regulations Regarding Obtaining Information From or Records of Members of the News Media; and Regarding Questioning, Arresting, or Charging Members of the News Media (Oct. 26, 2022), https://s3.documentcloud.org/documents/23199931/ag_memo_media_policy_20221026.pdf. The regulations apply to efforts to seek testimony, physical documents, telephone records, metadata, and digital content. 28 C.F.R. § 50.10(b)(2)(i).

[269] *See* 28 C.F.R. § 50.10(b)(3) &), *id.* § 50.10(d).

[270] *Id.* § 50.10(d).

[271] *Id.* § 50.10(b)(2)(ii).

[272] *See id.* § 50.10(e). When there is a close or novel question as to whether or entity is a member of the news media or acting within the scope of newsgathering, the determination of must be approved by the Assistant Attorney General for the Criminal Division. *Id.* When the Assistant Attorney General finds there is "genuine uncertainty" as to whether a member of the news media is engaged in newsgathering, the Attorney General must approve the determination concerning newsgathering. *Id.* § 50.10(e)(2).

[273] *See id.* § 50.10(b)(3).

[274] *See, e.g.*, Lee C. Bollinger and Geoffrey R. Stone, *Opening Statement*, in LEE C. BOLLINGER AND GEOFFREY R. STONE, NATIONAL SECURITY, LEAKS, AND FREEDOM OF THE PRESS: THE PENTAGON PAPERS FIFTY YEARS ON 264 (2021), at xv ("One of the most vexing and perennial questions facing any democracy is how to balance the government's legitimate need to conduct its operations—especially those related to protecting national security—with the public's right and responsibility to know what the government is doing.").

[275] *See* sources cited *supra* note 17.

[276] *See, e.g.*, House Judiciary WikiLeaks Hearing, *supra* note 215.

would prefer to keep out of view.[277] Some Members of Congress have sought to repeal or amend the Espionage Act to address these criticisms.[278]

The proposed Espionage Act Reform Act of 2022, introduced in the 117th Congress, for example, would have limited elements of the Espionage Act to those who receive official access to classified information, such as government employees and contractors.[279] This change would have altered the Espionage Act so that some provisions applied only to the individual responsible for the initial unauthorized disclosure, not to an individual or organization that receives leaks and publishes them.[280] Some commentators have argued that the press and other online platforms too frequently publish classified information and that the Espionage Act should be amended to more clearly apply to both the originators and the recipients of leaks.[281] Still others have argued that Congress should modify the executive branch's classification system and create more avenues to challenge classification decisions and make documents publicly available.[282]

Legislative proposals have also addressed DOJ's media policies and ability to obtain evidence from members of the press. Introduced in the 117th Congress, the Protect Reporters from Exploitative State Spying (PRESS) Act would have placed limitations on the United States' ability to compel disclosure of information that reveals a journalist's source or records that were obtained or created while engaging in journalism.[283] The Free Flow of Information Act, introduced most recently in the 115th Congress, would have defined the conditions under which the United States can compel a member of the media to provide testimony or documents related to information gained while engaging in journalism.[284]

Author Information

Stephen P. Mulligan
Legislative Attorney

Jennifer K. Elsea
Legislative Attorney

[277] *See id*.

[278] *See*, *e.g.*, @RandPaul, TWITTER (May 12, 2022, 11:02 AM), https://twitter.com/RandPaul/status/1558579480171614209 ("It is long past time to repeal [the Espionage Act].... ").

[279] Espionage Act Reform Act of 2022, H.R. 8533, 117th Cong. § 2 (2022).

[280] The proposed act would have allowed prosecutions against those who did not have official access to classified information (e.g., those outside government that received classified information) if the accused "directly and materially aids, or procures in exchange for anything of monetary value, the commission of an [Espionage Act] offense ... with the specific intent" to harm the United States or benefit a foreign government to the United States' detriment. *Id.*

[281] *See* Louis Michael Siedman, *Leaks in the Age of Trump*, *in* NATIONAL SECURITY, LEAKS, AND FREEDOM OF THE PRESS, *supra* note 274, at 264.

[282] *See*, *e.g.*, Report of the Commission, *in* NATIONAL SECURITY, LEAKS, AND FREEDOM OF THE PRESS, *supra* note 274, at 275–78 (collecting the recommendations from a five-person "Commission" on addressing leaks comprised of government officials, academics, and journalists). *See also* Modernizing the Government's Classification System, Hearing Before S. Comm. Homeland Sec. and Gov't Aff., 118th Cong. (2023), https://www.hsgac.senate.gov/hearings/modernizing-the-governments-classification-system/ (discussing avenues to reduce over-classification, increase transparency, and improve the classification process).

[283] *See* PRESS Act, H.R. 4330, 117th Cong. § 3 (2022).

[284] *See* Free Flow of Information Act of 2017, H.R. 4382, 115th Cong. § 2 (2017).

Disclaimer