Order Code RL33502

CRS Report for Congress

Protection of National Security Information

Updated December 26, 2006

Jennifer K. Elsea
Legislative Attorney
American Law Division

Prepared for Members and
Committees of Congress

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
26 DEC 2006	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Protection of National Security Information	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Library of Congress Congressional Research Service Washington, DC**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**SAR**	**27**	

Protection of National Security Information

Summary

Recent cases involving alleged disclosures of classified information to the news media or others who are not entitled to receive it have renewed Congress's interest with regard to the possible need for legislation to provide for criminal punishment for the "leaks" of classified information. The Espionage Act of 1917 and other statutes and regulations provide a web of authorities for the protection of various types of sensitive information, but some have expressed concern that gaps in these laws may make prosecution of some disclosures impossible. The 106th Congress passed a measure to criminalize leaks, but President Clinton vetoed it. The 108th Congress reconsidered the same provision, but instead passed a requirement for the relevant agencies to review the need for such a proscription. The Department of Justice in turn reported that existing statutes and regulations are sufficient to prosecute disclosures of information that might harm the national security.

This report provides background with respect to previous legislative efforts to criminalize the unauthorized disclosure of classified information; describes the current state of the laws that potentially apply, including criminal and civil penalties that can be imposed on violators; and some of the disciplinary actions and administrative procedures available to the agencies of federal government that have been addressed by federal courts. Finally, the report considers the possible First Amendment implications of applying the Espionage Act to prosecute newspapers for publishing classified national defense information.

Contents

Protection of National Security Information

Introduction

Continued revelations involving alleged disclosures of classified information to the news media or to others who are not entitled to receive it have renewed Congress's interest with regard to the possible need for legislation to provide for criminal punishment for the "leaks" of classified information. Opponents of any such legislation express concern regarding the possible consequences to freedom of the press and other First Amendment values. The current laws for protecting classified information have been criticized as a patchwork of sometimes abstruse and antiquated provisions that are not consistent and do not cover all the information the government legitimately needs to protect.[1] Certain information is protected regardless of whether it belongs to the government or is subject to normal classification. Information related to "the national defense" is protected even though no harm to the national security is intended or is likely to be caused through its disclosure. However, nonmilitary information with the potential to cause serious damage to the national security is only protected from willful disclosure with the requisite intent or knowledge regarding the potential harm. For example, under 50 U.S.C. § 783, the communication of classified information by a government employee is expressly punishable only if the discloser knows or has reason to believe the recipient is an

---

[1] *See* E.E.B. and K.E.M., Note, *Plugging the Leak: The Case for a Legislative Resolution of the Conflict between the Demands of Secrecy and the Need for Open Government*, 71 VA. L. REV. 801, 811 (1985). With respect to a major component of the legal framework, one district court judge had the following to say:

> The conclusion that the statute is constitutionally permissible does not reflect a judgment about whether Congress could strike a more appropriate balance between these competing interests, or whether a more carefully drawn statute could better serve both the national security and the value of public debate. Indeed, the basic terms and structure of this statute have remained largely unchanged since the administration of William Howard Taft. The intervening years have witnessed dramatic changes in the position of the United States in world affairs and the nature of threats to our national security. The increasing importance of the United States in world affairs has caused a significant increase in the size and complexity of the United States' military and foreign policy establishments, and in the importance of our nation's foreign policy decision making. Finally, in the nearly one hundred years since the passage of the Defense Secrets Act mankind has made great technological advances affecting not only the nature and potential devastation of modern warfare, but also the very nature of information and communication. These changes should suggest to even the most casual observer that the time is ripe for Congress to engage in a thorough review and revision of these provisions to ensure that they reflect both these changes, and contemporary views about the appropriate balance between our nation's security and our citizens' ability to engage in public debate about the United States' conduct in the society of nations.

United States v. Rosen, 445 F.Supp.2d 602, 646 (E.D. Va. 2006)(Ellis, J.).

agent or representative of a foreign government, but not, for example, if the recipient is an agent of an international terrorist organization.

To close some perceived gaps, the 106th Congress passed a measure to criminalize all leaks of classified information; however, President Clinton vetoed the measure.[2] The 108th Congress considered passing an identical provision as part of the Intelligence Authorization Act for Fiscal Year 2001,[3] but instead directed the Attorney General and heads of other departments to undertake a review of the current protections against the unauthorized disclosure of classified information, and to issue a report recommending legislative or administrative actions by May 1, 2002.[4] In its response to Congress, the Department of Justice concluded that existing statutes and regulations are sufficient to prosecute disclosures of information that might harm the national security.[5]

This report describes the current state of the law with regard to the unauthorized disclosure of classified information, including criminal and civil penalties that can be imposed on violators, as well as some of the disciplinary actions and administrative procedures available to federal agencies with respect to their employees, as such measures have been addressed by federal courts. The report also describes the background of legislative efforts to amend the laws, including the measure passed in 2000 and President Clinton's stated reasons for vetoing it. Finally, the report considers possible constitutional issues — in particular, issues related to the First Amendment — that may arise if Congress considers new legislation to punish leaks or if the Attorney General seeks to apply current law to punish newspapers that publish leaked classified information.

Background

The classification by government agencies of documents deemed sensitive has evolved from a series of executive orders.[6] Congress has, for the most part, let the executive branch make decisions regarding the type of information to be subject to protective measures. The current criminal statutory framework providing penalties for the unauthorized disclosure of classified government materials traces its roots to

---

[2] H.R. 4392 § 304, 106th Congress; *See* Statement by the President to the House of Representatives, 36 WEEKLY COMP. PRES. DOC. 278 (Nov. 4, 2000).

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

[4] *See* Intelligence Authorization Act for Fiscal Year 2002, P.L. 107-108, § 310 (2001). An identical measure was introduced in the 109th Congress, S. 3774, but was not reported out of committee.

[5] Letter from John Ashcroft, Attorney General of the United States, to Congress, October 15, 2002, *reported* 148 CONG. REC. S11,732 (daily ed. Nov. 20, 2002), *available online at* [http://www.fas.org/sgp/othergov/dojleaks.html](Last visited June 29, 2006).

[6] *See* SENATE COMM'N ON PROTECTING AND REDUCING GOVERNMENT SECRECY, 103d CONG., REPORT PURSUANT TO PUBLIC LAW 236 (Comm. Print 1997); CRS Report RS21900, *The Protection of Classified Information: The Legal Framework*, by Jennifer K. Elsea.

the Espionage Act of 1917,[7] which made it a crime to disclose defense information during wartime.[8] The National Security Act of 1947[9] directed the Director of the CIA to protect "intelligence sources and methods."[10] The Atomic Energy Act of 1954[11] provided for secrecy of information related to nuclear energy and weapons.[12] The Invention Secrecy Act of 1951[13] gave the government the authority to declare a patent application secret if disclosure of an invention might expose the country to harm.

Criminal Statutes for the Protection of Classified Information. National defense information is protected by the Espionage Act, 18 U.S.C. § 793 *et seq*. The penalty for violation of 18 U.S.C. § 793 (gathering, transmitting, or losing defense information) is a fine or imprisonment for not more than 10 years, or both. Thus, under § 793, persons convicted of gathering defense information with the intent or reason to believe the information will be used against the United States or to the benefit of a foreign nation may be fined or sentenced to no more than 10 years imprisonment.[14] Persons who have access to *defense* information that they have

---

[7] Act of June 15, 1917, ch. 30, title I, §§ 1, 6, 40 Stat. 217, 219, codified as amended at 18 U.S.C. §§ 793 *et seq*.

[8] *See* Anthony R. Klein, Comment, *National Security Information: Its Proper Role and Scope in a Representative Democracy*, 42 FED. COMM. L.J. 433, 437(1990) (describing evolution of anti-espionage laws).

[9] Codified at 50 U.S.C. § 401 *et seq*.

[10] 50 U.S.C. § 403(g).

[11] Codified at 42 U.S.C. § 2271 *et seq*. The dissemination of certain unclassified information related to nuclear facilities may be restricted by the Secretary of Energy pursuant to 42 U.S.C. § 2168 upon a finding that dissemination "could reasonably be expected to result in a significant adverse effect on the health and safety of the public or the common defense and security...." 42 U.S.C. § 2168(a)(4)(B).

[12] *See* Benjamin S. DuVal, Jr., *The Occasions of Secrecy*, 47 U. PITT. L. REV. 579, 596 (1986) (detailing restrictions directed at protecting nuclear secrets, or "Restricted Data").

[13] Codified at 35 U.S.C. § 181 *et seq*.

[14] 18 U.S.C. § 793(a)-(c) provides:

> (a) Whoever, for the purpose of obtaining information respecting the national defense with intent or reason to believe that the information is to be used to the injury of the United States, or to the advantage of any foreign nation, goes upon, enters, flies over, or otherwise obtains information concerning any vessel, aircraft, work of defense, [etc.], or any prohibited place so designated by the President by proclamation in time of war or in case of national emergency in which anything for the use of the Army, Navy, or Air Force is being prepared or constructed or stored, information as to which prohibited place the President has determined would be prejudicial to the national defense; or
>
> (b) Whoever, for the purpose aforesaid, and with like intent or reason to believe, copies, takes, makes, or obtains, or attempts to copy, take, make, or obtain any sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, document, writing, or note of anything connected with the national defense; or

(continued...)

reason to know could be used to harm the national security, whether the access is authorized or unauthorized, and who disclose that information to any person not entitled to receive it, or willfully retain the information despite an order to surrender it to an officer of the United States, are subject to the same penalty.[15] Although it is not necessary that the information be classified by a government agency, the courts give deference to the executive determination of what constitutes "defense information."[16] Information that is made available by the government to the public is not covered under the prohibition, however, because public availability of such

---

[14] (...continued)

> (c) Whoever, for the purpose aforesaid, receives or obtains or agrees or attempts to receive or obtain from any person, or from any source whatever, any [protected thing] connected with the national defense, knowing or having reason to believe. . . that it has been or will be obtained, taken, made, or disposed of by any person contrary to the provisions of this chapter [18 U.S.C. §§ 792 *et seq*.];....

[15] 18 U.S.C. § 793(d)-(f) provides:

> (d) Whoever, lawfully having possession of, access to, control over, or being entrusted with any document [or other protected thing] relating to the national defense, or information relating to the national defense . . . the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits . . . to any person not entitled to receive it, or willfully retains the same and fails to deliver it on demand to the officer or employee of the United States entitled to receive it; or
>
> (e) Whoever having unauthorized possession of, access to, or control over any document [or other protected thing], or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits . . . to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it; or
>
> (f) Whoever, being entrusted with or having lawful possession or control of any document [or other protected thing], or information, relating to the national defense,
>
> > (1) through gross negligence permits the same to be removed from its proper place of custody or delivered to anyone in violation of his trust, or to be lost, stolen, abstracted, or destroyed, or
> >
> > (2) having knowledge that the same has been illegally removed from its proper place of custody or delivered to anyone in violation of his trust, or lost, or stolen, abstracted, or destroyed, and fails to make prompt report of such loss, theft, abstraction, or destruction to his superior officer —
>
> Shall be fined under this title or imprisoned not more than ten years, or both.

[16] *See* United States v. Morison, 844 F.2d 1057 (4th Cir.), *cert. denied*, 488 U.S. 908 (1988)(upholding conviction under 18 U.S.C. § 793 for delivery of classified photographs to publisher).

information negates the bad-faith intent requirement.[17] On the other hand, classified documents may remain within the ambit of the statute even if information contained therein is made public by an unauthorized leak.[18] Any person who is lawfully entrusted with defense information and who permits it to be disclosed or lost, or who does not report such a loss or disclosure, is also subject to a penalty of up to 10 years in prison. The act covers information transmitted orally as well as information in tangible form.[19]

18 U.S.C. § 794 (aiding foreign governments) provides for imprisonment for any term of years or life, or under certain circumstances, the death penalty.[20] The provision penalizes anyone who transmits defense information to a foreign

---

[17] Gorin v. United States, 312, U.S. 9, 27-28 (1941) ("Where there is no occasion for secrecy, as with reports relating to national defense, published by authority of Congress or the military departments, there can, of course, in all likelihood be no reasonable intent to give an advantage to a foreign government.").

[18] United States v. Squillacote, 221 F.3d 542, 578 (4th Cir. 2000). *But see* United States v. Rosen, 445 F.Supp.2d 602, 620 (E.D. Va. 2006) (interpreting the reference in *Squillacote* to apply not to the document at issue, but rather, to information pertaining to the government's assessment of the validity of the information contained in it).

[19] United States v. Rosen, 445 F.Supp.2d 602, 616 (E.D. Va. 2006).

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

> (a) Whoever, with intent or reason to believe that it is to be used to the injury of the United States or to the advantage of a foreign nation, communicates, delivers, or transmits. . . to any foreign government, or to any faction or party or military or naval force within a foreign country, whether recognized or unrecognized by the United States, or to any representative, officer, agent, employee, subject, or citizen thereof, either directly or indirectly, any document [or other protected thing], or information relating to the national defense, shall be punished by death or by imprisonment for any term of years or for life, except that the sentence of death shall not be imposed unless the jury or . . . the court, further finds that the offense resulted in the identification by a foreign power (as defined in section 101(a) of the Foreign Intelligence Surveillance Act of 1978 [50 U.C.S. § 1801(a)]) of an individual acting as an agent of the United States and consequently in the death of that individual, or directly concerned nuclear weaponry, military spacecraft or satellites, early warning systems, or other means of defense or retaliation against large-scale attack; war plans; communications intelligence or cryptographic information; or any other major weapons system or major element of defense strategy.
>
> (b) Whoever, in time of war, with intent that the same shall be communicated to the enemy, collects, records, publishes, or communicates, or attempts to elicit any information with respect to the movement, numbers, description, condition, or disposition of any of the Armed Forces, ships, aircraft, or war materials of the United States, or with respect to the plans or conduct, or supposed plans or conduct of any naval or military operations, or with respect to any works or measures undertaken for or connected with, or intended for the fortification or defense of any place, or any other information relating to the public defense, which might be useful to the enemy, shall be punished by death or by imprisonment for any term of years or for life....

government (or certain other foreign entities) with the intent or reason to believe it will be used against the United States. The death penalty is available only upon a finding that the offense resulted in the death of a covert agent or directly concerns nuclear weapons or other particularly sensitive types of information. The death penalty is also available under §794 for violators who gather or transmit information related to military plans and the like during time of war, with the intent that the information reach the enemy.[21] Offenders are also subject to forfeiture of any ill-gotten gains and property used to facilitate the offense.[22]

Members of the military[23] who commit espionage, defined similarly to the conduct prohibited in 18 U.S.C. § 794, may be tried by court-martial for violating Article 106a of the Uniform Code of Military Justice (UCMJ),[24] and sentenced to

---

[21] During time of war, any individual who communicates intelligence or any other information to the enemy may be prosecuted by the military for aiding the enemy under Article 104 of the Uniform Code of Military Justice (UCMJ), and if convicted, punished by "death or such other punishment as a court-martial or military commission may direct." 10 U.S.C. § 904. Persons convicted by a general court-martial or by a military commission for "lurking as a spy or acting as a spy in or about any place, vessel, or aircraft, [etc.]" during time of war are to be punished by death. 10 U.S.C. § 906. Alien unlawful combatants within the meaning of chapter 47A of title 10, who, "with intent or reason to believe that it is to be used to the injury of the United States or to the advantage of a foreign power, collects or attempts to collect information by clandestine means or while acting under false pretenses, for the purpose of conveying such information to an enemy of the United States, or one of the co-belligerents of the enemy, shall be punished by death or such other punishment as a military commission ... may direct." 10 U.S.C.A. § 950v(27).

[22] 18 U.S.C. § 794(d). Proceeds go to the Crime Victims Fund.

[23] 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.

[24] 10 U.S.C. § 906a(a) provides:

Art. 106a. Espionage

> (a)(1) Any person subject to [the UCMJ, chapter 47 of title 10, U.S.C.] who, with intent or reason to believe that it is to be used to the injury of the United States or to the advantage of a foreign nation, communicates, delivers, or transmits, or attempts to communicate, deliver, or transmit, to any entity described in paragraph (2), either directly or indirectly, anything described in paragraph (3) shall be punished as a court-martial may direct, except that if the accused is found guilty of an offense that directly concerns (A) nuclear weaponry, military spacecraft or satellites, early warning systems, or other means of defense or retaliation against large scale attack, (B) war plans, (C) communications intelligence or cryptographic information, or (D) any other major weapons system or major element of defense strategy, the accused shall be punished by death or such other punishment as a court- martial may direct.

(continued...)

death if certain aggravating factors are found by unanimous determination of the panel.[25] Unlike offenses under § 794, Article 106a offenses need not have resulted in the death of a covert agent or involve military operations during war to incur the death penalty. One of the aggravating factors enabling the imposition of the death penalty under Article 106a is that "[t]he accused has been convicted of another offense involving espionage or treason for which either a sentence of death or imprisonment for life was authorized by statute."

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.[26] Violators are subject to fine or imprisonment for not more than one year, or both.

---

[24] (...continued)

(2) An entity referred to in paragraph (1) is —

(A) a foreign government;
(B) a faction or party or military or naval force within a foreign country, whether recognized or unrecognized by the United States; or
(C) a representative, officer, agent, employee, subject, or citizen of such a government, faction, party, or force.

(3) A thing referred to in paragraph (1) is a document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, note, instrument, appliance, or information relating to the national defense.

[25] 10 U.S.C. § 906a(b)-(c).

[26] § 795. Photographing and sketching defense installations

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

§ 797. Publication and sale of photographs of defense installations

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

The knowing and willful disclosure of certain classified information is punishable under 18 U.S.C. § 798 by fine and/or imprisonment for not more than 10 years.[27] To incur a penalty, the disclosure must be prejudicial to the safety or interests of the United States or work to the benefit of any foreign government and to the detriment of the United States. The provision applies only to information related to cryptographic systems and information related to communications intelligence specially designated by a U.S. government agency for "limited or restricted dissemination or distribution."[28] The provision protects information obtained by method of communications intelligence only if the communications were intercepted from a "foreign government," which, while broadly defined, may not include a transnational terrorist organization.[29]

18 U.S.C. § 641 punishes the theft or conversion of government property or records for one's own use or the use of another. While this section does not explicitly prohibit disclosure of classified information, it has been used for that purpose.[30] Violators may be fined, imprisoned for not more than 10 years, or both,

---

[27] § 798. Disclosure of classified information

> (a) Whoever knowingly and willfully communicates, furnishes, transmits, or otherwise makes available to an unauthorized person, or publishes, or uses in any manner prejudicial to the safety or interest of the United States or for the benefit of any foreign government to the detriment of the United States any classified information —
>
> (1) concerning the nature, preparation, or use of any code, cipher, or cryptographic system of the United States or any foreign government; or
>
> (2) concerning the design, construction, use, maintenance, or repair of any device, apparatus, or appliance used or prepared or planned for use by the United States or any foreign government for cryptographic or communication intelligence purposes; or
>
> (3) concerning the communication intelligence activities of the United States or any foreign government; or
>
> (4) obtained by the processes of communication intelligence from the communications of any foreign government, knowing the same to have been obtained by such processes —
>
> Shall be fined under this title or imprisoned not more than ten years, or both.

[28] 18 U.S.C. § 798(b).

[29] *Id*. ("The term 'foreign government' includes in its meaning any person or persons acting or purporting to act for or on behalf of any faction, party, department, agency, bureau, or military force of or within a foreign country, or for or on behalf of any government or any person or persons purporting to act as a government within a foreign country, whether or not such government is recognized by the United States.").

[30] *See* United States v. Morison, 844 F.2d 1057 (4th Cir. 1988)(photographs and reports were tangible property of the government); United States v. Fowler, 932 F.2d 306 (4th Cir. 1991)("information is a species of property and a thing of value" such that "conversion and

(continued...)

unless the value of the property does not exceed the sum of $100, in which case the maximum prison term is one year.

18 U.S.C. § 952 punishes employees of the United States who, without authorization, willfully publish or furnish to another any official diplomatic code or material prepared in such a code, by imposing a fine, a prison sentence (up to 10 years), or both. The same punishment applies for materials "obtained while in the process of transmission between any foreign government and its diplomatic mission in the United States."[31]

18 U.S.C. § 1030(a)(1) punishes the willful retention, communication, or transmission, etc., of classified information retrieved by means of knowingly accessing a computer without (or in excess of) authorization, with reason to believe that such information "could be used to the injury of the United States, or to the advantage of any foreign nation." The provision imposes a fine or imprisonment for not more than ten years, or both, in the case of a first offense or attempted violation. Repeat offenses or attempts can incur a prison sentence of up to twenty years.

18 U.S.C. § 1924 prohibits the unauthorized removal of classified material.[32] The provision imposes a fine of up to $1,000 and a prison term up to one year for government officers or employees who knowingly take material classified pursuant to government regulations with the intent of retaining the materials at an unauthorized location.[33]

---

[30] (...continued)
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).

[31] 18 U.S.C. § 952.

[32] 18 U.C.S. § 1924 provides:

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

[33] *Id.*

42 U.S.C. § 2274 punishes the unauthorized communication by anyone of "Restricted Data,"[34] or an attempt or conspiracy to communicate such data, by imposing a fine of not more than $500,000, a maximum life sentence in prison, or both, if done with the intent of injuring the United States or to secure an advantage to any foreign nation.[35] An attempt to disclose or participate in a conspiracy to disclose restricted data with the belief that such data will be used to injure the United States or to secure an advantage to a foreign nation, is punishable by imprisonment for no more than 10 years, a fine of no more than $100,000, or both.[36] The disclosure of "Restricted Data" by an employee or contractor, past or present, of the federal government to someone not authorized to receive it is punishable by a fine of not more than $12,500.[37]

50 U.S.C. § 421 provides for the protection of information concerning the identity of covert intelligence agents.[38] Any person authorized to know the identity of such agents who intentionally discloses the identity of a covert agent is subject to imprisonment for not more than 10 years or a fine or both.[39] A person who learns the identity of an agent through authorized access to classified information[40] and discloses the agent's identity to someone not authorized to receive classified information is subject to a fine, a term of imprisonment not more than five years, or both. 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

---

[34] The term "Restricted Data" is defined by the Atomic Energy Act of 1954 to include "all data concerning (1) design, manufacture, or utilization of atomic weapons; (2) the production of special nuclear material; or (3) the use of special nuclear material in the production of energy, but shall not include data declassified or removed from the Restricted Data category pursuant to [42 U.C.S. § 2162]." 42 U.C.S. § 2014(y).

[35] 42 U.S.C. § 2274(a). Receipt or tampering with Restricted Data with like intent is punishable in the same way under 42 U.S.C. §§ 2275 and 2276.

[36] 42 U.S.C. § 2274(b).

[37] 42 U.S.C. § 2277.

[38] The Intelligence Identities and Protection Act of 1982, codified at 50 U.S.C. §§ 421-26. For more information, see CRS Report RS21636, *Intelligence Identities Protection Act*, by Elizabeth B. Bazan.

[39] 50 U.S.C. § 421(a) provides:

> (a) Whoever, having or having had authorized access to classified information that identifies a covert agent, intentionally discloses any information identifying such covert agent to any individual not authorized to receive classified information, knowing that the information disclosed so identifies such covert agent and that the United States is taking affirmative measures to conceal such covert agent's intelligence relationship to the United States, shall be fined under title 18, United States Code, or imprisoned not more than ten years, or both.

[40] "Classified Information" is defined in 50 U.S.C. § 426(1) as "information or material designated and clearly marked or clearly represented, pursuant to the provisions of a statute or Executive order (or a regulation or order issued pursuant to a statute or Executive order), as requiring a specific degree of protection against unauthorized disclosure for reasons of national security."

any individual not authorized access to classified information, with reason to believe that such activities would impair U.S. foreign intelligence efforts, is subject to a fine or imprisonment for a term of not more than three years. To be convicted, a violator must have knowledge that the information identifies a covert agent whose identity the United States is taking affirmative measures to conceal. An agent is not punishable under this provision for revealing his or her own identity, and it is a defense to prosecution if the United States has already publicly disclosed the identity of the agent.[41]

50 U.S.C. § 783 penalizes government officers or employees who, without proper authority, communicate classified information to a person whom the employee has reason to suspect is an agent or representative of a foreign government.[42] It is also unlawful for the representative or agent of the foreign government to receive classified information.[43] Violation of either of these provisions is punishable by a fine of up to $10,000 or imprisonment for not more than 10 years.[44] Violators are

---

[41] *See* Lawrence P. Gottesman, Note, *The Intelligence Identities Protection Act of 1982: An Assessment of the Constitutionality of Section 601(c)*, 49 BROOKLYN L. REV. 479, 483 - 485 (1983)(outlining the elements of an offense under 50 U.S.C. § 421).

[42] 50 U.S.C. § 783(a) provides:

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

[43] 50 U.S.C. 783(b) provides:

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

[44] 50 U.S.C. § 783(c).

thereafter prohibited from holding public office.[45] 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.[46]

Disclosure of a patent that has been placed under a secrecy order pursuant to the Invention Secrecy Act of 1951[47] can result in a fine of $10,000, imprisonment for up to two years, or both. Publication or disclosure of the invention must be willful and with knowledge of the secrecy order to be punishable.[48]

Civil Penalties and Other Measures. In addition to the criminal penalties outlined above, the executive branch employs numerous means of deterring unauthorized disclosures by government personnel using administrative measures based on terms of employment contracts.[49] The agency may impose disciplinary action or revoke a person's security clearance.[50] The revocation of a security clearance is usually not reviewable by the Merit System Protection Board[51] and may mean the loss of government employment. Government employees may be subject to monetary penalties for disclosing classified information.[52] Violators of the Espionage Act and the Atomic Energy Act provisions may be subject to loss of their retirement pay.[53]

Agencies also rely on contractual agreements with employees, who typically must sign non-disclosure agreements prior to obtaining access to classified information,[54] sometimes agreeing to submit all materials that the employee desires to publish to a review by the agency. The Supreme Court enforced such a contract against a former employee of the Central Intelligence Agency (CIA), upholding the

---

[45] *Id.*

[46] 50 U.S.C. § 783(e).

[47] Codified at 35 U.S.C. § 181 *et seq*.

[48] 35 U.S.C. § 186.

[49] *See* DuVal, *supra* note 12, at 597 (identifying administrative regulations as principal means of enforcing secrecy procedures).

[50] *See, e.g.*, Exec. Order 12,958. Sanctions may include "reprimand, suspension without pay, removal, ... loss or denial of access to classified information, or other sanctions in accordance with applicable law and agency regulation." *Id.* at §5.7(c).

[51] *See* Department of Navy v. Egan, 484 U.S. 518, 526-29 (1988). Federal courts may review constitutional challenges based on the revocation of security clearance. Webster v. Doe, 486 U.S. 592 (1988).

[52] *See* 42 U.S.C. § 2282(b) (providing for fine of up to $100,000 for violation of Department of Energy security regulations).

[53] 5 U.C.S. § 8312 (2001)(listing violations of 18 U.S.C. §§ 793 & 798, 42 U.S.C. § 2272-76, and 50 U.S.C. § 421, among those for which forfeiture of retirement pay or annuities may be imposed).

[54] *See* United States v. Marchetti, 466 F.2d 1309 (4th Cir.), *cert. denied,* 409 U.S. 1063 (1972) (enforcing contractual non-disclosure agreement by former employee regarding "secret information touching upon the national defense and the conduct of foreign affairs" obtained through employment with CIA).

government's imposition of a constructive trust on the profits of a book the employee sought to publish without first submitting it to CIA for review.[55]

In 1986, the Espionage Act was amended to provide for the forfeiture of any property derived from or used in the commission of an offense.[56] Violators of the Atomic Energy Act may be subjected to a civil penalty of up to $100,000 for each violation of Energy Department regulations regarding dissemination of unclassified information about nuclear facilities.[57]

The government can also use injunctions to prevent disclosures of information. The courts have generally upheld injunctions against former employees' publishing information they learned through access to classified information.[58] The Supreme Court also upheld the State Department's revocation of passports for overseas travel by persons planning to expose U.S. covert intelligence agents, despite the fact that the purpose was to disrupt U.S. intelligence activities rather than to assist a foreign government.[59]

Similarly, the government can enjoin publication of inventions when it is determined that the release of such information is detrimental to the national security. If an inventor files a patent application for an invention that the Commissioner of Patents believes should not be made public, the Commissioner may place a secrecy order on the patent and establish conditions for granting a patent, or may withhold grant of a patent as long as the "national interest requires [it]."[60] In addition to criminal penalties cited previously, in the case of an unauthorized disclosure or foreign filing of the patent information, the Patent Office will deem the invention to be "abandoned," which means a forfeiture by the applicant, his successors, or assigns of all claims against the United States based on the invention.[61]

The government has had less success trying to enjoin the media from disclosing classified information. Most famously, the government failed to enjoin publication of the Pentagon Papers by a newspaper, even though the information was clearly classified and had been stolen by someone with access to it.[62] In that case, the Supreme Court set very high standards for imposing prior restraint on the press. Yet

---

[55] *See* Snepp v. United States, 444 U.S. 507 (1980); s*ee also* Alan E. Garfield, *Promises of Silence: Contract Law and Freedom of Speech,* 83 CORNELL L. REV. 261, 274 (1998)(noting the remedy in *Snepp* was enforced despite the agency's stipulation that the book did not contain any classified information).

[56] *See* 18 U.S.C. §§ 793(h), 794(d), 798(d); Klein, *supra* note 8, at 438-439.

[57] 42 U.S.C. § 2168(b).

[58] *See* United States v. Marchetti, 466 F.2d 1309 (4th Cir. 1972) (granting an injunction to prevent a former CIA agent from publishing a book disclosing government secrets).

[59] *See* Haig v. Agee, 453 U.S. 280 (1981).

[60] 35 U.S.C. § 181. The determination must be renewed on a yearly basis.

[61] 35 U.S.C. § 182.

[62] United States v. New York Times, 403 U.S. 713 (1971). *See* Klein, *supra* note 8, at 439-40.

in another case, the government was able to enjoin a newspaper from printing information about the design of an atomic bomb, even though the information did not originate from classified material and the author's purpose was not subversive.[63]

Prior Legislative Efforts

The current laws for protecting classified information have been criticized as a patchwork of provisions that are not consistent and do not cover all the information the government legitimately needs to protect.[64] Certain information is protected regardless of whether it belongs to the government or is subject to normal classification. Technical and scientific information, for example, can be restricted regardless of source.[65] Information related to "the national defense" is protected even though no harm to the national security is intended or is likely to be caused through its disclosure. However, nonmilitary information with the potential to cause serious damage to the national security is only protected from willful disclosure with the specific intent to harm the national interest,[66] or with the knowledge that such harm could occur.[67]

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

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

---

[63] *See* DuVal, *supra* note 12, at 604 (describing Progressive magazine article at issue in United States v. Progressive, Inc., 467 F.Supp. 990 (W.D. Wis. 1979)); Klein, *supra* note 8, at 435 (noting disparity between rulings in *New York Times* and *Progressive*). The information the Progressive sought to publish was related to the building of a nuclear bomb and was thus classified as "Restricted Data" under the Atomic Energy Act, even though the information had been compiled from unclassified, publicly available documents. One reason for the different outcomes in the two cases is that the Atomic Energy Act contains statutory authorization for the Attorney General to seek injunction. *See* 42 U.S.C. § 2280. In *New York Times*, a majority of Justices took into account the fact that Congress had not authorized an injunction. 403 U.S. at 718 (Black, J., concurring); *id*. at 721-22 (Douglas, J., concurring); *id*. at 730 (Stewart, J., concurring); *id*. at 731-40 (White, J., concurring); *id.* at 742 (Marshall, J., concurring).

[64] *See* E.E.B. and K.E.M., Note, *Plugging the Leak: The Case for a Legislative Resolution of the Conflict between the Demands of Secrecy and the Need for Open Government*, 71 VA. L. REV. 801, 811 (1985).

[65] *See id.* at 814.

[66] *See id.* at 815.

[67] *See* United States v. Morison, 844 F.2d 1057 (1988).

The new provision would have penalized the disclosure of any material designated as classified for any reason related to national security, regardless of whether the violator intended that the information be delivered to and used by foreign agents (in contrast to 50 U.S.C. § 783). It would have been the first law to penalize disclosure of information to entities other than foreign governments or their equivalent solely because it is classified, without a more specific definition of the type of information covered.[68] In short, the provision would have made it a crime to disclose or attempt to disclose classified information[69] to any person who does not have authorized access to such information, with exceptions covering disclosures to Article III courts, or to the Senate or House committees or Members, and for authorized disclosures to persons acting on behalf of a foreign power (including an international organization). The provision would have amended the espionage laws in title 18 by expanding the scope of information they cover. The proposed language was intended to make it easier for the government to prosecute unauthorized disclosures of classified information, or "leaks" of information that might not amount to a violation of current statutes. The language was intended to ease the government's burden of proof in such cases by eliminating the need "to prove that damage to the national security has or will result from the unauthorized disclosure,"[70] substituting a requirement to show that the unauthorized disclosure was of information that "is or has been properly classified" under a statute or executive order.

The 106th Congress passed the measure,[71] but President Clinton vetoed it, calling it "well-intentioned" as an effort to deal with a legitimate concerns about the damage caused by unauthorized disclosures, but "badly flawed" in that it was "overbroad" and posed a risk of "unnecessarily chill[ing] legitimate activities that are at the heart of a democracy."[72] The President explained his view that

> [a] desire to avoid the risk that their good faith choice of words — their exercise of judgment — could become the subject of a criminal referral for prosecution might discourage Government officials from engaging even in appropriate public

---

[68] 18 USCS § 1924 prohibits removal of government-owned or controlled classified information by a government employee without authorization. 50 U.S.C. § 783 covers only information classified by the President or an executive agency transmitted by a government employee to a foreign government. 18 U.S.C. §§ 793 and 794 are potentially broader than these in that they cover information "related to the national defense," by government employees and others without regard to the identity of the recipient of the information, but these require intent or knowledge regarding harm to the national defense.

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

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

[71] H.R. 4392 § 304, 106th Congress.

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

> discussion, press briefings, or other legitimate official activities. Similarly, the legislation may unduly restrain the ability of former Government officials to teach, write, or engage in any activity aimed at building public understanding of complex issues. Incurring such risks is unnecessary and inappropriate in a society built on freedom of expression and the consent of the governed and is particularly inadvisable in a context in which the range of classified materials is so extensive. In such circumstances, this criminal provision would, in my view, create an undue chilling effect.[73]

The 108th Congress considered passing an identical provision as part of the Intelligence Authorization Act for Fiscal Year 2001,[74] but instead directed the Attorney General and heads of other departments to undertake a review of the current protections against the unauthorized disclosure of classified information, and to issue a report recommending legislative or administrative actions.[75] An identical measure was introduced late in the 109th Congress, but was not reported out of committee.[76]

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

> [a]lthough there is no single statute that provides criminal penalties for all types of unauthorized disclosures of classified information, unauthorized disclosures of classified information fall within the scope of various current statutory criminal prohibitions. It must be acknowledged that there is no comprehensive statute that provides criminal penalties for the unauthorized disclosure of classified information irrespective of the type of information or recipient involved. Given the nature of unauthorized disclosures of classified information that have occurred, however, I conclude that current statutes provide a legal basis to prosecute those who engage in unauthorized disclosures, if they can be identified. It may be that carefully drafted legislation specifically tailored to unauthorized disclosures of classified information generally, rather than to espionage, could enhance our investigative efforts. The extent to which such a provision would yield any practical additional benefits to the government in terms of improving our ability to identify those who engage in unauthorized disclosures of classified information or deterring such activity is unclear, however.[77]

Constitutional Issues

The publication of information pertaining to the national defense may serve the public interest by providing citizens with information necessary to shed light on the workings of government, but some observe a consensus that the public release of at least *some* defense information poses a significant enough threat to the security of the nation that the public interest is better served by keeping it secret. The Constitution protects the public right to access government information and to express opinions

---

[73] *Id.*

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

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

[76] S. 3774, 109th Cong.

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

regarding the functioning of the government, among other things, but it also charges the government with "providing for the common defense." Policymakers are faced with the task of balancing these interests.

The First Amendment to the U.S. Constitution provides: "Congress shall make no law ... abridging the freedom of speech, or of the press...."[78] Despite this absolute language, the Supreme Court has held that "[t]he Government may ... regulate the content of constitutionally protected speech in order to promote a compelling interest if it chooses the least restrictive means to further the articulated interest."[79]

First Amendment Principles. Where speech is restricted based on its content, the Supreme Court generally applies "strict scrutiny," which means that it will uphold a content-based restriction only if it is necessary "to promote a compelling interest," and is "the least restrictive means to further the articulated interest."[80]

Compelling Interest. Protection of the national security from external threat is without doubt a compelling government interest.[81] 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.[82] Speech likely to incite immediate violence, for example, may be suppressed.[83] Speech that would give military advantage to a foreign enemy is also susceptible to government regulation.[84]

Where First Amendment rights are implicated, it is the government's burden to show that its interest is sufficiently compelling to justify enforcement. Whether the government has a compelling need to punish disclosures of classified information turns on whether the disclosure has the potential of causing damage to the national

---

[78] For an analysis of exceptions to the First Amendment, see CRS Report 95-815, *Freedom of Speech and Press: Exceptions to the First Amendment*, by Henry Cohen.

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

[80] *Id.*

[81] *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., at 509; *accord* Cole v. Young, 351 U.S. 536, 546 (1956)).

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

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

[84] 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.").

defense or foreign relations of the United States.[85] Actual damage need not be proved, but potential damage must be more than merely speculative and incidental.[86]

Promotion of that Interest. In addition to showing that the stated interest to be served by the statute is compelling, the government must also show that the law actually serves that end. If the accused can show that the statute serves an unrelated purpose — for example, to silence criticism of certain government policies or to manipulate public opinion — a judge might be prepared to invalidate the statute.[87] If, for example, the government releases some positive results of a secret weapons program while suppressing negative results, a person prosecuted for releasing negative information could challenge the statute by arguing that his prosecution is related to the negative content of his speech rather than to valid concerns about the damage it might cause. If he can show that those who disclose sensitive information that tends to support the administration's position are not prosecuted, while those who disclose truthful information that is useful to its opponents are prosecuted, he might be able to persuade a court that the statute as enforced is an unconstitutional restriction of speech based on impermissible content-related interests.[88]

Least Restrictive Means. To survive a constitutional challenge, a law must be narrowly drawn to affect only the type of speech that the government has a compelling need to suppress.[89] A statute that reaches speech that the government has no sufficiently compelling need to regulate may be subject to attack due to overbreadth. A law is overly broad if it prohibits more speech than is necessary to achieve its purpose. If a defendant can show that a statute regulating speech is "substantially overbroad," he may challenge its validity on its face.[90] If the law is found to be substantially overbroad, a court will invalidate the law even if the defendant's conduct falls within the ambit of conduct that the government may

---

[85] "National Security" is defined as national defense and foreign relations. *See* Exec.Order No. 12,958, 60 Fed. Reg.19,825 (Apr. 17, 1995).

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

[87] In all likelihood, such a defendant would have to prove not only that such an impermissible use is possible, but also that it is pertinent to the particular case.

[88] *Cf.* R.A.V. v. City of St. Paul, 505 U.S. 377 (1992); *but see* Snepp v. United States, 444 U.S. 507 (1980)(Stevens, J., dissenting). Snepp's assertion of selective enforcement against his book based on its critical treatment of the CIA failed to persuade the Supreme Court that any violation of the First Amendment had occurred. *See* Judith Schenk Koffler and Bennett L. Gershman, *National Security and Civil Liberties: The New Seditious Libel*, 69 CORNELL L. REV. 816, 847 (1984).

[89] *See* E.E.B. and K.E.M., *supra* note 1, at 849.

[90] Broadrick v. Oklahoma, 413 U.S. 601 (1973).

legitimately prohibit. For this reason, a statute that relies solely on the Executive's classification of information to determine the need for its protection might be contested as overbroad.[91] If a challenger were able to show that agencies classify information that it is unnecessary to keep secret, he could argue that the statute is invalid as overly broad because it punishes protected speech that poses no danger to the national security.

Although information properly classified in accordance with statute or executive order carries by definition, if disclosed to a person not authorized to receive it, the potential of causing at least identifiable harm to the national security of the United States,[92] it does not necessarily follow that government classification by itself will be dispositive of the issue in the context of a criminal trial. Government classification will likely serve as strong evidence to support the contention. Typically, courts have been unwilling to review decisions of the executive related to national security, or have made a strong presumption that the material at issue is potentially damaging.[93] In the context of a criminal trial, especially in a case with apparent First Amendment implications, courts may be more willing to engage in an evaluation of the propriety

---

[91] Courts have rejected challenges of the Espionage Act based on overbreadth stemming from the imprecision of the term "information related to the national defense" by reading other requirements into the statute. *See, e.g.*, United States v. Rosen, 445 F.Supp.2d 602, 643 (E.D. Va. 2006)(rejecting overbreadth challenge on the basis of judicial interpretation of 18 U.S.C. § 793 that requires the government to prove "(1) that the information relates to the nation's military activities, intelligence gathering or foreign policy, (2) that the information is closely held by the government, in that it does not exist in the public domain; and (3) that the information is such that its disclosure could cause injury to the nation's security").

[92] Exec. Order No. 12,958, 60 Fed. Reg.19,825 (Apr. 17, 1995)("Classified National Security Information").

Sec. 1.3 defines three levels of classification:

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

(Emphasis added).

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

of a classification decision than they would in a case of citizens seeking access to information under the Freedom of Information Act (FOIA).[94]

The Supreme Court seems satisfied that national security is a vital interest sufficient to justify some intrusion into activities that would otherwise be protected by the First Amendment — at least with respect to federal employees. Although the Court has not held that government classification of material is sufficient to show that its release is damaging to the national security,[95] it has seemed to accept without much discussion the government's assertion that the material in question is damaging. Lower courts have interpreted 18 U.S.C. § 798, which criminalizes the unauthorized release of specific kinds of classified information,[96] to have no requirement that the government prove that the classification was proper or personally approved by the President.[97] It is unlikely that a defendant's bare assertion that information is unlikely to damage U.S. national security will be persuasive without some convincing evidence to that effect, or proof that the information is not closely guarded by the government.[98]

Snepp v. United States[99] affirmed the government's ability to enforce contractual non-disclosure agreements against employees and former employees who had had access to classified information. The Supreme Court allowed the government to impose a constructive trust on the earnings from Frank Snepp's book about the CIA because he had failed to submit it to the CIA for prepublication review, as he had agreed to do by signing an employment agreement. Although the CIA stipulated to the fact that the book contained no classified information,[100] the Court accepted the finding that the book caused "irreparable harm and loss" to the American intelligence services.[101] The Court suggested that the CIA did not need a signed agreement in

---

[94] 5 U.S.C. § 552(b)(1) exempts classified information from release to requesters.

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

[96] 18 U.S.C. § 798 provides in pertinent part:
"(a) Whoever knowingly and willfully communicates, furnishes, transmits, or otherwise makes available to an unauthorized person, ... any classified information ... (2) concerning the design, construction, use, maintenance, or repair of any device, apparatus, or appliance used or prepared or planned for use by the United States ... for cryptographic or communication intelligence purposes; ... (s)hall be fined ... or imprisoned ...."

[97] *See, e.g.* United States v. Boyce, 594 F.2d 1246, 1251 (9th Cir. 1979) ("Under section 798, the propriety of the classification is irrelevant. The fact of classification of a document or documents is enough to satisfy the classification element of the offense.").

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

[99] 444 U.S. 507 (1980).

[100] *Id.* at 511.

[101] *Id.* at 512.

order to protect its interests by subjecting its former employees to prepublication review and possible censorship.[102]

Haig v. Agee[103] was a First Amendment challenge to the government's ability to revoke a citizen's passport because of his intent to disclose classified information. Philip Agee was a former CIA agent who engaged in a "campaign to fight the United States CIA," which included publishing names of CIA operatives around the world. In order to put a stop to this activity, the Department of State revoked his passport. Agee challenged that action as an impermissible burden on his freedom to travel and an effort to penalize his exercise of free speech to criticize the government.[104] The Supreme Court disagreed, finding the passport regulations constitutional because they may be applied "only in cases involving likelihood of 'serious damage' to national security or foreign policy."[105]

United States v. Morison[106] is significant in that it represents the first case in which a person was convicted for selling classified documents to the media. Morison argued that the espionage statutes did not apply to his conduct because he could not have had the requisite intent to commit espionage. The Fourth Circuit rejected his appeal, finding the intent to sell photographs that he clearly knew to be classified sufficient to satisfy the scienter requirement under 18 U.S.C. § 793. The definition of "relating to the national defense" was not overbroad because the jury had been instructed that the government had the burden of showing that the information was so related.[107]

Prior Restraint. In addition to restricting the disclosure of information by prosecuting the person responsible after the fact, the government may seek to prevent publication by prior restraint (i.e., seeking a temporary restraining order or an injunction from a court to enjoin publication).[108] The Supreme Court, however, is unlikely to uphold such an order. It has written:

> [P]rior restraints are the most serious and least tolerable infringement on First Amendment rights.... A prior restraint, ... by definition, has an immediate and irreversible sanction. If it can be said that a threat of criminal or civil sanctions

---

[102] *Id.* at 509, n3 ("Moreover, 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")(citations omitted).

[103] 453 U.S. 280 (1981).

[104] *Id.* at 305.

[105] *Id.* at 305-06.

[106] 844 F.2d 1057 (4th Cir.), *cert. denied*, 488 U.S. 908 (1988).

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

[108] The Supreme Court struck down an injunction against publishing the Pentagon Papers, writing: "Any system of prior restraints of expression comes to the Court bearing a heavy presumption against its constitutional validity." New York Times Co. v. United States, 403 U.S. 713, 714 (1971).

> after publication "chills" speech, prior restraint "freezes" it at least for the time. The damage can be particularly great when the prior restraint falls upon the communication of news and commentary on current events.[109]

The government's ability to protect sensitive information was explored in the context of prior restraints of the media in the *Pentagon Papers* case.[110] In a *per curiam* opinion accompanied by nine concurring or dissenting opinions, the Court refused to grant the government's request for an injunction to prevent the *New York Times* and the *Washington Post* from printing a classified study of the U.S. involvement in Vietnam. A majority of the justices indicated in *dicta*, however, that the newspapers — as well as the former government employee who leaked the documents to the press — could be prosecuted under the Espionage Act.[111]

Due Process. A statute is unconstitutionally vague if it does not permit the ordinary person to determine with reasonable certainty whether his conduct is criminally punishable. Therefore, a statute prohibiting the unauthorized disclosure of classified information must be sufficiently clear to allow a reasonable person to know what conduct is prohibited. Where First Amendment rights are implicated, the concern that a vague statute will have a chilling effect on speech not intended to be covered may make that law particularly vulnerable to judicial invalidation.[112]

The Espionage Act of 1917[113] has been challenged for vagueness without success. There have been very few prosecutions under that act for disclosing information related to the national defense. The following elements are necessary to prove an unauthorized disclosure offense under 18 U.S.C. § 793:

> 1. The information or material disclosed must be related to the national defense, that is, pertaining to any matters "directly and reasonably connected with the defense of our nation against its enemies" that "would be potentially damaging to the United States, or might be useful to an enemy of the United States" and are "closely held" in that the relevant government agency has sought to keep them from the public generally and that these items have not been made public and are not available to the general public.[114]

---

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

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

[111] *See* David Topol, Note, *United States v. Morison: A Threat to the First Amendment Right to Publish Security Information*, 43 S.C. L. REV. 581, 586 (noting that six of the nine *Pentagon Papers* justices suggested that the government could convict the newspapers under the Espionage Act even though it could not enjoin them from printing the documents).

[112] *See* Aptheker v. Secretary of State, 378 U.S. 500 (1964); United States v. Robel, 389 U.S. 258 (1967); Smith v. Goguen, 415 U.S. 566, 573 (1974); Village of Shaumberg v. Citizens for a Better Environment, 444 U.S. 620 (1980).

[113] 18 U.S.C. § 793 *et seq.*

[114] *See* United States v. Morison, 622 F. Supp. 1009, 1010 (D. Md.1985).

2. The disclosure must be made with knowledge that such disclosure is not authorized.

3. There must be an "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.

There does not appear to be a requirement that the disclosure cause actual harm.[115] An evil motive is not necessary to satisfy the scienter requirement; the willfulness prong is satisfied by the knowledge that the information may be used to the injury of the United States.[116] It is irrelevant whether the information was passed to a *friendly* foreign nation.[117] A patriotic motive will not likely change the outcome.[118]

The Supreme Court, in *Gorin v. United States*,[119] upheld portions of the Espionage Act now codified as sections 793 and 794 of title 18, U.S. Code (communication of certain information to a foreign entity) against assertions of vagueness, but only because jury instructions properly established the elements of the crimes, including the scienter requirement and a definition of "national defense" that includes potential damage in case of unauthorized release of protected information and materials. *Gorin* was a "classic case" of espionage, and there was no challenge based on First Amendment rights. The Court agreed with the government that the term "national defense" was not vague; it was satisfied that it "is a generic concept of broad connotations, referring to the military and naval establishments and the related activities of national preparedness."[120] Whether information was "related to the national defense" was a question for the jury to decide,[121] based on its determination that the information "may relate or pertain to the usefulness, efficiency or availability of any of the above places, instrumentalities or things for the defense of the United States of America. The connection must not be a strained one nor an arbitrary one. The relationship must be reasonable and direct."[122] As long as the jury was properly instructed that information not likely to cause damage was not "related to the national defense" for the purpose of the statute, the term was not unconstitutionally vague.

No other challenge to a conviction under the Espionage Act has advanced to the Supreme Court.

---

[115] *See* United States v. Morison, 844 F.2d 1057, 1074 (4th Cir. 1988).

[116] *Id.* at 1073.

[117] Gorin v. United States, 312 U.S. 19, 29 (1941).

[118] United States v. Morison, 622 F.Supp. 1009 (D. Md. 1985).

[119] 312 U.S. 19 (1941).

[120] *Id.* at 28.

[121] *Id.* at 32.

[122] *Id.* at 31.

Conclusion

Under the present legal framework, the publication of national security information by non-government personnel may be prosecuted under various provisions, but only if the information meets the definition set forth by statute and the disclosure is made with the requisite knowledge or intent with regard to the nature of the damage it could cause. The First Amendment limits Congress's ability to prohibit the publication of information of value to the public, especially with regard to pre-publication injunctions against non-government employees. That the publication of some information has the potential to damage U.S. national security interests is rarely denied, but an agreement on how to protect such information without harming the public's right to know what its government is doing may remain elusive.