Order Code RL31245

Protection of National Security Information: The Classified Information Protection Act of 2001

January 16, 2002

Jennifer Elsea
Legislative Attorney
American Law Division

Protection of National Security Information: The Classified Information Protection Act of 2001

Summary

The purpose of this report is to identify legal issues relevant to legislation introduced in Congress that provides for criminal punishment for the unauthorized disclosure of classified information by government employees and contractors with access to such information. The Classified Information Protection Act of 2001, H.R. 2943, would make such an act a felony punishable by a fine or a prison term no longer than three years, or both.

The language in H.R. 2943 is identical to section 304 of H.R. 4392, 106th Congress, the Intelligence Authorization Act for Fiscal Year 2001. H.R. 4392 was passed by both Houses of Congress but vetoed by President Clinton, who cited section 304 as the reason for his veto. The Intelligence Authorization Act was then passed as H.R. 5630, P.L. 106-567, without the language of section 304. The stated purpose of section 304 was to stop "leaks" by public officials of sensitive national security information to the press, in an effort to prevent the compromise of intelligence sources and methods and other sensitive information in the open media.

This report will first describe H.R. 2943, the stated intent of the Congress in passing the measure as section 304 of the intelligence authorization bill for 2001, and President Clinton's stated reasons for vetoing it. The report will then describe the current state of the law with regard to the unauthorized disclosure of classified information, including criminal penalties that can be imposed upon violators; it will also discuss civil penalties, as well as some of the disciplinary actions and administrative procedures available to the agencies of federal government that have been addressed by federal courts, and will then assess any changes to the law that would result if the language of H.R. 2943 were enacted. Finally, the report will consider possible constitutional infirmities that might leave the law vulnerable to judicial intervention under the First Amendment, the Fifth Amendment, or the constitutional separation of powers between the President and Congress.

Contents

Protection of National Security Information: The Classified Information Protection Act of 2001

Introduction

The purpose of this report is to identify legal issues relevant to proposals providing criminal punishment for the unauthorized disclosure of classified information by government employees and contractors with access to such information. The Classified Information Protection Act of 2001, H.R. 2943, would make such an act a felony punishable by a fine or a prison term no longer than three years, or both.

The language in the Act is identical to section 304 of H.R. 4392, 106th Congress, the Intelligence Authorization Act for Fiscal Year 2001. H.R. 4392 was passed by both Houses of Congress but vetoed by President Clinton, who cited section 304 as the reason for his veto.[1] The Intelligence Authorization Act was then passed as H.R. 5630, P.L. 106-567, without the language of section 304. Congress later 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.[2]

This report will first describe H.R. 2943, the stated intent of the Congress in passing the measure as section 304 of the intelligence authorization bill for 2001, and President Clinton's stated reasons for vetoing it. The report will then describe the current state of the law with regard to the unauthorized disclosure of classified information, including criminal penalties that can be imposed upon violators; it will also discuss civil penalties, as well as some of the disciplinary actions and administrative procedures available to the agencies of federal government that have been addressed by federal courts, and will then assess any changes to the law that would result if the language of H.R. 2943 were enacted. Finally, the report will consider possible constitutional infirmities that might leave the law vulnerable to judicial intervention under the First Amendment, the Fifth Amendment, or the constitutional separation of powers between the President and Congress.

Provisions of the Act

H.R. 2943 would create 18 U.S.C. § 798A, subsection (a) of which would read:

---

[1] *See* Statement by the President to the House of Representatives, 36 WEEKLY COMP. PRES. DOC. 278 (Nov. 4, 2000).

[2] *See* Intelligence Authorization Act for Fiscal Year 2002, Pub. L. No. 107-108, § 310 (2001).

> 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.

In short, subsection (a) would make it a crime to disclose or attempt to disclose classified information to any person who does not have authorized access to such information. The remaining subsections would clarify the boundaries of the prohibitions in subsection (a). Subsection (b) of the legislation provides exceptions for 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). Subsection (c) defines terms used in the legislation. The definition of "classified information" covers both "properly classified" information which is "clearly marked or represented," and information which the person making or attempting to make the disclosure "knows or has a reason to believe has been properly classified by appropriate officials."[3] "Authorized" would mean "authority or permission to have access ... pursuant to the provisions of a statute, Executive order, regulation or directive," a court order, or Senate or House rules controlling classified information. "Officer or employee of the United States" would include the definitions set forth in 5 U.S.C. §§ 2104-05 as well as officers and enlisted members of the Armed Forces as defined in 10 U.S.C. § 101(b).

The language would amend the espionage laws in title 18 by expanding the scope of information they cover. The new language was originally intended to make it easier for the government to prosecute unauthorized disclosures of classified information, or "leaks" of information that might not amount to espionage under the 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."[4] The element of damage would be met by showing that the unauthorized disclosure was of information that "is or has been properly classified" under a statute or executive order.

---

[3]"Classified information" is fully defined as "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." "National Security" is defined as national defense and foreign relations. *See* Exec.Order No. 12,958, 60 Fed. Reg.19,825 (Apr. 17, 1995); 18 U.C.S. Appx § 1 (Classified Information Protection Act).

[4]*See* H.R. REP. NO. 106-969 at 44 (2000).

Background

The classification by government agencies of documents deemed sensitive has evolved from a series of executive orders.[5] 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 the Espionage Act of 1917,[6] which made it a crime to disclose defense information during wartime.[7] The National Security Act of 1947[8] directed the Director of the CIA to protect "intelligence sources and methods."[9] The Atomic Energy Act of 1954[10] provided for secrecy of information related to nuclear energy and weapons.[11] The Invention Secrecy Act of 1951[12] 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 18 U.S.C. § 793 *et seq*. The penalty for violation of 18 U.S.C. § 793 is a fine or imprisonment for not more than ten years, or both. 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 ten years imprisonment.[13] Persons who have access to *defense* information which they have

---

[5]*See* SENATE COMM'N ON PROTECTING AND REDUCING GOVERNMENT SECRECY, 103D CONG., REPORT PURSUANT TO PUBLIC LAW 236 (Comm. Print 1997).

[6] Codified at 18 U.S.C.§§ 793 *et seq*.

[7] *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).

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

[9]50 U.S.C. § 403(g).

[10]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).

[11]*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").

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

[13] 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, navy yard, naval station, submarine base, fueling station, fort, battery, torpedo station,
>
> (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.[14] Although it is

---

[13](...continued)

dockyard, canal, railroad, arsenal, camp, factory, mine, telegraph, telephone, wireless, or signal station, building, office, research laboratory or station or other place connected with the national defense owned or constructed, or in progress of construction by the United States or under the control of the United States, or of any of its officers, departments, or agencies, or within the exclusive jurisdiction of the United States, or any place in which any vessel, aircraft, arms, munitions, or other materials or instruments for use in time of war are being made, prepared, repaired, stored, or are the subject of research or development, under any contract or agreement with the United States, or any department or agency thereof, or with any person on behalf of the United States, or otherwise on behalf of the United States, or any prohibited place so designated by the President by proclamation in time of war or in case of national emergency in which anything for the use of the Army, Navy, or Air Force is being prepared or constructed or stored, information as to which prohibited place the President has determined would be prejudicial to the national defense; or

(b) Whoever, for the purpose aforesaid, and with like intent or reason to believe, copies, takes, makes, or obtains, or attempts to copy, take, make, or obtain any sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, document, writing, or note of anything connected with the national defense; or

(c) Whoever, for the purpose aforesaid, receives or obtains or agrees or attempts to receive or obtain from any person, or from any source whatever, any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note, of anything connected with the national defense, knowing or having reason to believe, at the time he receives or obtains, or agrees or attempts to receive or obtain it, 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.*];....

[14] 18 U.S.C. § 793(d)-(f) provides:

(d) Whoever, lawfully having possession of, access to, control over, or being entrusted with any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted or attempts to communicate, deliver, transmit or cause to be communicated, delivered or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it on demand to the officer or employee of the United States entitled to receive it; or

(e) Whoever having unauthorized possession of, access to, or control over any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note relating to the national defense, or information relating to the national defense which information the possessor

(continued...)

not necessary that the information be classified by a government agency, the courts give deference to the executive determination of what constitutes "defense information."[15] 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 ten years in prison.

18 U.S.C. § 794 provides for imprisonment for any term of years or life, or under certain circumstances, the death penalty.[16] The provision penalizes anyone who

---

[14](...continued)

has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it 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, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, note, or information, relating to the national defense, (1) through gross negligence permits the same to be removed from its proper place of custody or delivered to anyone in violation of his trust, or to be lost, stolen, abstracted, or destroyed, or (2) having knowledge that the same has been illegally removed from its proper place of custody or delivered to anyone in violation of his trust, or lost, or stolen, abstracted, or destroyed, and fails to make prompt report of such loss, theft, abstraction, or destruction to his superior officer--

Shall be fined under this title or imprisoned not more than ten years, or both.

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

[16] § 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, or attempts to communicate, deliver, or transmit, 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, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, note, instrument, appliance, 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, if there is no jury, 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.

(continued...)

transmits defense information to a foreign government (or other foreign entity) 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

---

[16](...continued)

(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.

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

(d) (1) Any person convicted of a violation of this section shall forfeit to the United States irrespective of any provision of State law--

(A) any property constituting, or derived from, any proceeds the person obtained, directly or indirectly, as the result of such violation, and

(B) any of the person's property used, or intended to be used, in any manner or part, to commit, or to facilitate the commission of, such violation. For the purposes of this subsection, the term "State" includes a State of the United States, the District of Columbia, and any commonwealth, territory, or possession of the United States.

(2) The court, in imposing sentence on a defendant for a conviction of a violation of this section, shall order that the defendant forfeit to the United States all property described in paragraph (1) of this subsection.

(3) The provisions of subsections (b), (c) and (e) through (p) of section 413 of the Comprehensive Drug Abuse Prevention and Control Act of 1970 (21 U.S.C. 853(b), (c), and (e)-(p)) shall apply to--

(A) property subject to forfeiture under this subsection;

(B) any seizure or disposition of such property; and

(C) any administrative or judicial proceeding in relation to such property, if not inconsistent with this subsection.

(4) Notwithstanding section 524(c) of title 28, there shall be deposited in the Crime Victims Fund in the Treasury all amounts from the forfeiture of property under this subsection remaining after the payment of expenses for forfeiture and sale authorized by law.

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.[17]

Members of the military[18] 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 UCMJ,[19] and sentenced to death if certain aggravating factors are found by unanimous determination of the panel.[20] Unlike offenses under § 794, Article

---

[17]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.

[18]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, and certain others with military status. 10 U.S.C. § 802.

[19] 10 U.S.C. § 906a(a) provides:

Art. 106a. Espionage

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

[20] 10 U.S.C. § 906a(b)-(c) provides:

(continued...)

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

---

[20](...continued)

(b)(1) No person may be sentenced by court-martial to suffer death for an offense under this section (article) unless--

(A) the members of the court-martial unanimously find at least one of the aggravating factors set out in subsection (c); and

(B) the members unanimously determine that any extenuating or mitigating circumstances are substantially outweighed by any aggravating circumstances, including the aggravating factors set out in subsection (c).

(2) Findings under this subsection may be based on--

(A) evidence introduced on the issue of guilt or innocence;

(B) evidence introduced during the sentencing proceeding; or

(C) all such evidence.

(3) The accused shall be given broad latitude to present matters in extenuation and mitigation.

(c) A sentence of death may be adjudged by a court-martial for an offense under this section (article) only if the members unanimously find, beyond a reasonable doubt, one or more of the following aggravating factors:

(1) The 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.

(2) In the commission of the offense, the accused knowingly created a grave risk of substantial damage to the national security.

(3) In the commission of the offense, the accused knowingly created a grave risk of death to another person.

(4) Any other factor that may be prescribed by the President by regulations under section 836 of this title (article 36).

prohibited by 18 U.S.C. §§ 795 and 797.[21] Violators are subject to fine or imprisonment for not more than one year, or both.

The knowing and willful disclosure of certain classified information is punishable under 18 U.S.C. § 798 by fine and/or imprisonment for not more than ten years.[22] To

---

[21] § 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.

(b) Whoever violates this section shall be fined under this title or imprisoned not more than one year, or both.

§ 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, 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 of the military or naval post, camp, or station concerned, 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.

[22] § 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

(continued...)

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."[23]

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.[24] Violators may be fined or imprisoned for not more than ten years or both, unless the value of the property does not exceed the sum of $100, in which case the maximum prison term is one year.

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 and up to ten years' prison sentence, 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."[25]

---

[22](...continued)

> (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.

[23]18 U.S.C. § 798(b).

[24]*See* United States v. Morison, 844 F.2d 1057 (4th Cir. 1988)(photographs and reports were tangible property of the government); United States v. Fowler, 932 F.2d 306 (4th Cir. 1991)("information is a species of property and a thing of value" such that "conversion and conveyance of governmental information can violate § 641,"citing United States v. Jeter, 775 F.2d 670, 680-82 (6th Cir. 1985)); United States v. Girard, 601 F.2d 69, 70-71 (2d Cir. 1979).

[25]18 U.S.C. § 952.

18 U.S.C. § 1924 prohibits the unauthorized removal of classified material.[26] 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.[27]

42 U.S.C. § 2274 punishes the unauthorized communication by anyone of "Restricted Data,"[28] or an attempt or conspiracy to communicate such data, by imposing a fine of not more than $500,000 and 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.[29] A disclosure, attempt to disclose or participation in a conspiracy to disclose restricted data with the belief that such data will be utilized to injure the United States or secure an advantage to a foreign nation is punishable by imprisonment for no more than ten years or a fine of no more than $100,000, or both.[30] 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.[31]

---

[26]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.

[27]*Id.*

[28]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).

[29]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.

[30]42 U.S.C. § 2274(b).

[31]42 U.S.C. § 2277.

50 U.S.C. § 421 provides for the protection of information concerning the identity of covert intelligence agents.[32] 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 ten years or a fine, or both.[33] A person who learns the identity of an agent through authorized access to classified information[34] and discloses the agent's identity to someone not authorized to receive classified information is subject to a fine or 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 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.[35]

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.[36] It is

---

[32] The Intelligence Identities and Protection Act of 1982, codified at 50 U.S.C. §§ 421-26.

[33] 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.

[34] "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."

[35] *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).

[36] 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

(continued...)

also unlawful for the representative or agent of the foreign government to receive classified information.[37] Violation of either of these provisions is punishable by a fine of up to $10,000 or imprisonment for not more than 10 years.[38] Violators are thereafter prohibited from holding public office.[39] Violators must forfeit all property derived directly or indirectly from the offense and any property which was used or intended to be used to facilitate the violation.[40]

Disclosure of a patent which has been placed under a secrecy order pursuant to the Invention Secrecy Act of 1951[41] can lead to a fine of $10,000 or 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.[42]

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.[43]

---

[36](...continued)

> 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.

[37] 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.

[38]50 U.S.C. § 783(c).

[39]*Id.*

[40]50 U.S.C. § 783(e).

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

[42]35 U.S.C. § 186.

[43]*See* DuVal, *supra* note 11, at 597 (identifying administrative regulations as principal means of enforcing secrecy procedures).

The agency may impose disciplinary action or revoke a person's security clearance.[44] The revocation of a security clearance is usually not reviewable by the Merit System Protection Board[45] and may mean loss of government employment. Government employees may be subject to other monetary penalties for disclosing classified information.[46] Violators of the Espionage Act and the Atomic Energy Act provisions may be subject to loss of their retirement pay.[47]

Agencies also rely on contractual agreements with employees, who typically must sign non-disclosure agreements prior to obtaining access to classified information,[48] sometimes agreeing to submit all materials which 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, upholding the 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.[49]

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.[50] 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.[51]

The government can also use injunctions to prevent disclosures of information. The courts have generally upheld injunctions against former employees' publishing

---

[44]*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).

[45]*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).

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

[47]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).

[48]*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).

[49] *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).

[50]*See* 18 U.S.C. §§ 793(h), 794(d), 798(d); Klein, *supra* note 7, at 438-439.

[51]42 U.S.C. § 2168(b).

information they learned through access to classified information.[52] 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 assist a foreign government.[53]

Similarly, the government can enjoin publication of inventions when it is determined that release of such information is detrimental to the national security. If an inventor files a patent application for an invention the Commissioner of Patents believes should not be made public, the Commissioner may place a secrecy order on the patent and may establish conditions for granting a patent, or may withhold grant of a patent as long as the "national interest requires [it]."[54] 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.[55]

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.[56] In that case, the Supreme Court set very high standards for imposing prior restraint on the press. Yet 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.[57]

---

[52]*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).

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

[54]35 U.S.C. § 181. The determination must be renewed on a yearly basis.

[55]35 U.S.C. § 182.

[56]United States v. New York Times, 403 U.S. 713 (1971). *See* Klein, *supra* note 7, at 439-40.

[57]*See* DuVal, *supra* note 11, 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 7, 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).

H.R. 2943 and Current Law.

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.[58] 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.[59] 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,[60] or with the knowledge that such harm could occur.[61]

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. It would be the first law to penalize disclosure of information to non-foreign entities solely because it is classified, without a more specific definition of the type of information covered.[62]

Constitutional Issues

The First Amendment to the U.S. Constitution provides: "Congress shall make no law . . . abridging the freedom of speech, or of the press . . . ." 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."[63] The constitutionality of section 304, therefore, if enacted and challenged in court, will depend upon whether the government can demonstrate that the statute promotes a compelling interest and does so by the least restrictive means available.

---

[58]*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).

[59]*See id.* at 814.

[60]*See id.* at 815.

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

[62]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 entity.

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

First Amendment Principles.

Compelling Interest.

Protection of the national security from external threat is without doubt a compelling government interest.[64] Particularly during time of war or heightened risk of hostilities, it has long been accepted that the government has a compelling need to suppress certain types of speech.[65] Speech likely to incite immediate violence, for example, may be suppressed.[66] Speech that would give military advantage to a foreign enemy is also susceptible to government regulation.[67]

Where First Amendment rights are implicated, it is the government's burden to show that its interest is sufficiently compelling to justify enforcement. Whether the government has a compelling need to punish disclosures of classified information turns on whether the disclosure has the potential of causing damage to the national defense or foreign relations of the United States.[68] Actual damage need not be proved, but potential damage must be more than merely speculative and incidental.[69]

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.[70] A challenge could be brought against section 304 charging that, under certain circumstances, the government uses

---

[64]*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)).

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

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

[67] 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.").

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

[69]*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)).

[70] 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.

its classification procedures to suppress certain speech. Such a challenge might evolve in a case of alleged selected release of information on the part of the government related to sensitive government programs. If the government releases some positive results of a secret weapons program while suppressing negative results, for example, 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.[71]

Another argument along these lines would note that a statute that prohibits disclosure of classified information, but fails to prohibit the disclosure of sensitive but unclassified information, leaves significant vulnerabilities, calling into question the relationship between the law's means and ends. Also, a defendant might argue that the statute is underinclusive because the conduct is only punishable if perpetrated by someone with authorized access to the classified information. Arguably, if the disclosure of the information is damaging, it would be irrelevant how or by whom it was disclosed.[72] Lastly, a person challenging the statute could argue that the statute does not sufficiently address circumstances in which the potential damage to the national security is outweighed by other considerations.

Least Restrictive Means.

To survive a constitutional challenge, the law must be narrowly drawn to affect only the type of speech that the government has a compelling need to suppress.[73] If the statute reaches speech that the government has no sufficiently compelling need to regulate, the statute will 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.[74] 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 the government may legitimately prohibit. For this reason, the statute might be contested as overbroad by virtue of its reliance on the Executive's classification scheme. If a challenger were able to show that agencies classify

---

[71]*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).

[72]On the other hand, the government has a greater interest in restricting the speech of its employees than it does with respect to the public at large. Pickering v. Board of Education, 391 U.S. 563, 568 (1968).

[73]*See* E.E.B. and K.E.M., *supra* note 58, at 849.

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

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,[75] it does not necessarily follow that government classification by itself will be dispositive of the issue in the context of a criminal trial. In other words, courts may interpret the language of the proposed statute to impose on the government the burden of showing that the disclosure at issue has (or had at the time of its unauthorized release) the potential of harming national security.[76] Government classification will likely serve as strong evidence to support the contention, but it is unlikely the accused will be foreclosed entirely from bringing a First Amendment challenge to the government's assertion that potential damage to the national security is likely.

Information may be properly classified in the technical sense – that is, the appropriate authority determined it met specific criteria for classification of material that could cause the requisite level of damage to the United States if it falls into the wrong hands, and yet for other reasons, that information could be judged to pose no realistic threat. For example, a defendant could argue that the information she is charged with releasing is already widely available in public sources and therefore has already caused any damage it was capable of causing. Or she may argue that the information was properly classified at the time of its creation but is now so old that no foreign entity could possibly benefit from learning about it. A defendant might even argue that limited release unlikely to cause direct and imminent injury to the United States was necessary to avert greater harm to life and limb of innocent persons.

---

[75]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).

[76]The Committee Report suggests that *proper* classification by itself should discharge the government's burden. H.R. REP. NO. 106-969 at 44 (2000).

Therefore, one issue that is almost certain to arise, if this statute is enacted, is the extent to which the judiciary should defer to the judgment of the executive in determining whether an unauthorized disclosure of classified information has the potential to cause harm to the national security. 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.[77] 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 of a classification decision than they would in a case of citizens seeking access to information under the Freedom of Information Act (FOIA).[78]

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,[79] 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,[80] to have no requirement that the government prove that the classification was proper or personally approved by the President.[81] 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.[82]

Snepp v. United States[83] 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

---

[77]*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.").

[78]5 U.S.C. § 552(b)(1) exempts classified information from release to requesters.

[79]*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).

[80]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 . . .".

[81] *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.").

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

[83]444 U.S. 507 (1980).

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,[84] the Court accepted the finding that the book caused "irreparable harm and loss" to the American intelligence services.[85] The Court suggested that the CIA did not need a signed agreement in order to protect its interests by subjecting its former employees to prepublication review and possible censorship.[86]

Haig v. Agee[87] 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.[88] 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."[89]

United States v. Morison[90] 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.[91]

---

[84]*Id.* at 511.

[85]*Id.* at 512.

[86]*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).

[87]453 U.S. 280 (1981).

[88]*Id.* at 305.

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

[90]844 F.2d 1057 (4th Cir.), *cert. denied,* 488 U.S. 908 (1988).

[91]*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).

The government's ability to protect sensitive information was explored in the context of prior restraints of the media in the *Pentagon Papers Case*.[92] 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.[93]

If strictly construed to mean that the government, in order to prove its compelling need to suppress disclosure of classified information, need only show that the proper procedures were followed in applying the classification, the proposed legislation would raise concerns of overbreadth under the First Amendment. However, for precisely this reason it may not be so strictly construed.[94]

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.[95]

The Espionage Act of 1917 has been challenged for vagueness without success. There have been very few prosecutions 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

---

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

[93]*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).

[94]*See, e.g.* United States v. X-Citement Video, 513 U.S. 64 (1994).

[95]*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).

generally and that these items have not been made public and are not available to the general public.[96]

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.[97] 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.[98] It is irrelevant whether the information was passed to a *friendly* foreign entity.[99] A patriotic motive will not likely change the outcome.[100]

Sections 793 and 794 (communication of certain information to a foreign entity) have survived challenges for 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. The Supreme Court case relied upon for these standards is *Gorin v. United States*,[101] which interpreted the predecessor statutes to §§ 793 and 794. *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."[102] Whether information was "related to the national defense" was a question for the jury to decide,[103] 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."[104] 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.

---

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

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

[98] *Id.* at 1073.

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

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

[101] 312 U.S. 19 (1941).

[102] *Id.* at 28.

[103] *Id.* at 32.

[104] *Id.* at 31.

The definition of the term "classified information" in the proposed statute may invite challenge on the grounds that it is vague. The definition of "classified" under the section is ambiguous, as it includes the words it is intended to define. It applies to information "classified" pursuant to statutes and executive orders as requiring protection from unauthorized dissemination for reasons of national security. Clearly, it applies to the national security designations under Executive Order 12,958.[105] It probably applies to "Restricted Data" under title 42, the dissemination of which is already punishable. It could be construed to apply to the "unclassified" information that is protected under 42 U.S.C. §§ 2167-68, because such information may be regulated to prohibit unauthorized dissemination if the Secretary of Energy determines such dissemination "could reasonably be expected to result in a significant adverse effect on ... the common defense and security ...."[106] Section 304 also appears to apply to classified information that is not owned or controlled by the government, and does not appear to make an exception for information that was properly classified but has since been declassified, or should be declassified according to agency rules.

Classified information includes "information or material properly classified and clearly marked or represented, or that the person knows or has reason to believe has been properly classified by appropriate authorities, pursuant to the provisions of a statute or Executive order, as requiring protection against unauthorized disclosure for reasons of national security." Whether a government employee has reason to believe certain material "has been properly classified" may under some circumstances be difficult to establish. Government officials sometimes may be required to guess whether a piece of information falls under an agency's classification guidelines, for instance, if it appears in some context without proper classification markings.

Classification guidelines are to some extent discretionary, so that not all information meeting the criteria for classification will in fact be classified. Information that is classified in one document should be marked as classified in every document in which it appears, but references to classified information may not always be properly marked, or might be presented in such a way that gives rise to questions about whether it should be classified in its new form. Documents that contain secrets may also contain unclassified information. Secret information may be spoken and thus carry no clear classification markings to give notice to the recipient. Information may require classification under one agency's guidelines but remain unprotected under the guidelines of another agency. These factors arguably present vagueness issues because of the danger of chilling protected speech about unclassified matter. Some critics contend that employees who are unsure whether information is or should be classified may keep silent rather than risk disclosing any fact they could be deemed to have had "reason to believe" is or has been properly classified.

---

[105]60 Fed. Reg.19,825 (Apr. 17, 1995)(defining levels of classification). *See supra*,note 75.

[106]42 U.S.C. § 2168(a)(4)(B).

The language "for reasons of national security" invites challenge because the term "national security" is arguably so broad as to invite claims of vagueness.[107] However, a review of pertinent case law reveals that courts do not seem to have been overly troubled by the breadth or ambiguity of the term.[108]

The fact that the proposed law applies only to government employees or "other person[s] with access to classified information" may help to immunize it from claims of vagueness, since presumably those with access to classified information have a greater understanding of the applicable classification rules[109] and have agreed to abide by them.[110]

It should probably be remembered that challenges to the statute as enforced, even if successful, are unlikely to render the statute unconstitutional on its face. If a statute can be interpreted in such a way as to avoid unconstitutional results, courts will interpret it that way.[111] Government employees who clearly understand the damaging potential of information and leak it anyway will not likely succeed in an attempt to get the law declared unconstitutional based on the possible chilling effect the statute may have on hypothetical violators. However, due process will require that any defendant faced with a criminal penalty be allowed to present credible evidence that the law is vague or that the government does not have a compelling need to suppress the speech that forms the basis for the charge against him.

Separation of Powers.

Some concern has been raised in the media with respect to the proposed legislation, i.e. that allowing the executive branch to in effect both promulgate and enforce criminal statutes amounts to a violation of the constitutional scheme for making laws. Because the proposed statute ratifies and enforces the Executive Order governing classified information without providing standards to guide the classification process, it may be argued by some that the Congress is delegating its lawmaking authority entirely to the executive branch. It is urged that, particularly where a statute imposes a criminal penalty on violators, a strong system of checks and balances is vital to ensuring fundamental liberties.

There is little precedent to support invalidating the proposed legislation on the basis of an alleged violation of separation of powers. The Constitution contains no explicit separation of powers doctrine; the theory derives from the first three Articles

---

[107]*See* E.E.B. and K.E.M., *supra* note 58, at 852 (citing McGehee v. Casey, 718 F.2d 1137 (D.C. Cir. 1983)).

[108]*See* Gorin v. United States, 312 U.S. 19, 27 (1941) (finding in the term "national defense" no "uncertainty which deprives a person of the ability to predetermine whether a contemplated action is criminal under the provisions of this law"); United States v. Dedeyan, 594 F.2d 36, 39-40 (4th Cir. 1978) (finding that delimitation in jury instruction removed any vagueness) (citing *Gorin*); McGehee v. Casey, 718 F.2d 1137 (D.C. Cir. 1983).

[109]Scarbeck v. United States, 317 F.2d 546, 548 (D.C. Cir. 1962).

[110]Snepp v. United States, 444 U.S. 507 (1980)(per curiam).

[111]United States v. X-Citement Video, 513 U.S. 64, 68-69 (1994).

and their allocation of powers among the three branches of government. The related concept of checks and balances reflects wisdom on the part of the Framers that the system would be stronger if each of the branches had a role in countermanding or approving the actions of the other two. In practice, the executive and judicial branches have each been permitted to exercise powers that are seemingly legislative in nature, provided such powers are delegated by Congress.[112]

Congress may delegate broad responsibilities to the President so long as it lays down an "intelligible principle" to guide the rule-making authority.[113] Opponents of the proposed legislation may argue that the statute does not contain an intelligible principle because it relies on principles established by Executive order that could change without congressional influence. However, the Supreme Court has long approved delegations accompanied by very general legislative guidance.[114] That information must be properly classified "pursuant to the provisions of a statute or Executive order, as requiring protection against unauthorized disclosure for reasons of national security" arguably serves as sufficient guidance for delegation purposes.

The executive branch has long been recognized as holding especially strong sway in the realm of foreign affairs and national defense. The courts have accepted that the President has the power to classify information vital to national security as a part of his powers as Commander-in-Chief.[115] The Court has honored Congress' desire to give deference to the Executive in matters of classification.[116] In light of this power, and evidence that Congress has approved of its use and supplemented it through various statutes, it is highly unlikely that a challenge based on a separation of powers claim would succeed.

---

[112]For example, the so-called independent regulatory agencies may carry out functions that are executive (law enforcement), legislative (rulemaking) or judicial (adjudicatory) in nature.

[113]*See* Touby v. United States, 500 U.S. 160 (1990) (citing Lichter v. United States, 334 U.S. 742 (1948).

[114]*See Touby* at 165 (finding "imminent hazard to the public safety" standard to be intelligible for the purposes of criminal sanctions).

[115]Department of the Navy v. Egan, 484 U.S. 518 (1988).

[116]EPA v. Mink, 410 U.S. 73 (1973).