ValpoScholar Valparaiso University Law Review

Volume 42
Number 4 *Symposium: Unethical Says Who?: A Look at How People and Institutions Help Businesses Fulfill Their Ethical Obligations*

*pp.*1277-1317

Symposium: Unethical Says Who?: A Look at How People and Institutions Help Businesses Fulfill Their Ethical Obligations

Someone Talked! The Necessity of Prohibitions Against Publishing Classified Financial Intelligence Information

Mark R. Alson

Note

SOMEONE TALKED![1] THE NECESSITY OF PROHIBITIONS AGAINST PUBLISHING CLASSIFIED FINANCIAL INTELLIGENCE INFORMATION

I. INTRODUCTION

For a moment, imagine a nightmare scenario for this nation.[2] The terrorist organization al Qaeda, never quenching in its appetite for the destruction of America by ruthlessly murdering her civilians, acquires a nuclear weapon after purchasing it from a rogue nation such as Iran or North Korea. The purchase involves millions of dollars, accumulated from various donations, "charities," and other gifts from entities that support al Qaeda's objectives. The funds, normally held in European bank accounts subject to tracking, are instead clandestinely held and physically carried by persons and entities throughout the United States, Europe, and the Middle East, eventually getting to terrorist leaders in Pakistan. The funds are given to the rogue nation in exchange for the nuclear suitcase bomb.

The nuclear weapon is transported via numerous al Qaeda operatives onto a ship in the French port of Marseilles. The ship, normally carrying only legitimate exports, sails to the port of Miami, where the container carrying the weapon is smuggled. The container is placed on a semi-truck and driven by a terrorist operative to Washington, D.C. Upon arrival, a sleeper cell hides the bomb and awaits a message from terrorist leaders overseas for the date of detonation. Families of the sleeper cell, still living in the Middle East, each have been given thousands of dollars; a few years ago, the money would have been extracted from an al Qaeda bank account and digitally transferred to the families' bank accounts. Instead, the money is physically handed over.

---

[1] A portion of the title of this Note is a reproduction of a famous World War II poster slogan, depicting a drowning sailor. The National Archives, http://www.archives.gov/research/ww2/photos/images/ww2-26.jpg (last visited Mar. 7, 2008) (for an illustration of the poster).

[2] This scenario is a hypothetical invented by the author.

Throughout the multiple month process of planning and executing the plot, thousands of communications have occurred. In the recent past, many of the contacts with the sleeper cell in America would have been sent though e-mails and telephone calls. However, in this case, the communications occur by persons flying to and from Europe, where operatives meet in safe houses. The few e-mails that are sent are encrypted in elaborate code.

At a final meeting at a safe house in Europe, a member of the sleeper cell is told of the date of the proposed attack in Washington, a communication that may have previously occurred by a telephone communication. A week later, the attack occurs, killing hundreds of thousands of civilians and government employees, causing billions of dollars of damage, and causing unfathomable grief to families and strangers alike throughout America and around the world.

While the preceding scenario is frightening to imagine, such plots may be in the planning stages by those persons who spend every waking moment designing ways to destroy the United States. Each step of the scheme involves secrecy and silence, a difficult task to accomplish, especially if al Qaeda does not know America's tactics of detecting the terrorist organization's operations. However, now imagine that the terrorists have learned of two of the most top secret methods that America currently uses to foil terrorist plots. They have gained this knowledge neither through spies embedded in the State Department, nor by blackmailing families of government leaders, but rather by simply reading the front pages of major American newspapers. The reader need not imagine this portion of the scenario, for it has already occurred.[3]

Currently, the Federal Criminal Code includes two provisions that attempt to prohibit certain classified information from being published, the Espionage Act and the COMINT statute.[4] However, the language and legislative history of the Espionage Act are difficult to fully understand, and such ambiguity causes it to be ineffective as it relates to disclosures through publishing.[5] Additionally, the COMINT statute, while explicitly outlawing the publication of certain communications intelligence, is too narrow to encompass other classified intelligence disclosures, the secrecy of which are crucial to national security interests.[6] Therefore, this Note proposes an additional provision to the

---

3 *See infra* Part II.E.

4 *See infra* Parts II.A-B.

5 *See infra* Part III.A.

6 *See infra* note 37 for full text of the statute.

Federal Criminal Code that would prohibit the publishing of classified information which relates to the financial intelligence activities of the United States.[7]

This Note explores the balance between freedom of the press and necessary legislation to counter fears that some published information may harm national security, and whether such laws should be enforced and updated. Part II of this Note examines the history of current laws such as the Espionage Age and the COMINT statute, the subsequent enforcement of those laws, and the actions of the *New York Times* that may have violated those statutes.[8] Next, Part III inspects whether the Espionage Act or COMINT statutes are sufficiently comprehensible to encompass the articles published by the *Times* and whether public policy considerations sanction such a prosecution.[9] Furthermore, Part IV proposes additional necessary legislation that would encompass disclosures related to the financial activities of the United States against which current laws do not protect.[10]

II. BACKGROUND

The balance between protecting confidential national security information and the public's right to know has undergone various adjustments throughout this country's history, especially as foreign affairs transformed. Part II.A explores the evolution of the Espionage Act's creation, with particular emphasis not only on its legislative history and the historic events that led to its enactment, but also the Act's ambiguity.[11] Juxtaposing those provisions, Part II.B presents the COMINT statute, including an analysis of its language and legislative intent.[12] Next, Part II.C examines the extent to which the Pentagon Papers case affects current assessments of the prohibitions on the publication of national security information.[13] Then, Part II.D considers subsequent judicial decisions that have reinforced the importance of national security secrecy and trends towards its protection.[14] Finally, Part II.E reviews the *New York Times'* recent disclosures of the government's program to monitor international communications

---

7 *See infra* Part IV.
8 *See infra* Part II.
9 *See infra* Part III.
10 *See infra* Part IV.
11 *See infra* Part II.A.
12 *See infra* Part II.B.
13 *See infra* Part II.C.
14 *See infra* Part II.D.

without a court warrant, as well as its program of tracking terrorist financial activity.[15]

A. The Espionage Act

To fully understand the meaning and potential application of 18 U.S.C. § 798, one must first grasp the way in which the fragile balance between national security secrets and the freedoms of speech and press have garnered attention in the legislative branch. For much of this nation's history, people who engaged in unauthorized disclosures of government secrets were punished under general statutes regarding treason, unlawful entry into military bases, and theft of government property.[16] Thereafter, Congress directly considered the issue of protecting government secrets in the early twentieth century when it passed the Defense Secrets Act of 1911 ("DSA").[17] The DSA, which was a

---

[15] *See infra* Part II.E.

[16] Harold Edgar & Benno C. Schmidt, Jr., *The Espionage Statutes and Publication of Defense Information*, 73 COLUM. L. REV. 929, 940 (1973) (describing in much detail the federal espionage statutes, focusing on how the Espionage Act's language is difficult to fully understand, and concluding that the basic espionage statutes are insufficiently drafted).

[17] Edgar & Schmidt, *supra* note 16, at 939-40 (quoting 36 Stat. 1804 (1911)). The statute provides:

> SEC. 1. That whoever, for the purpose of obtaining information respecting the national defense, to which he is not lawfully entitled, goes upon any vessel, or enters any navy-yard, naval station, fort, battery, torpedo station, arsenal, camp, factory, building, office, or other place connected with the national defense, owned or constructed or in process of construction by the United States, or in the possession or under the control of the United States or any of its authorities or agents, and whether situated within the United States or in any place non-contiguous to but subject to the jurisdiction thereof; or whoever, when lawfully or unlawfully upon any vessel, or in or near any such place, without proper authority, obtains, takes, or makes, or attempts to obtain, take, or make, any document, sketch, photograph, photographic negative, plan, model, or knowledge of anything connected with the national defense to which he is not entitled; or whoever, without proper authority, receives or obtains, or undertakes or agrees to receive or obtain, from any person, any such document, sketch, photograph, photographic negative, plan, model, or knowledge, knowing the same to have been so obtained, taken or made; or whoever, having possession of or control over any such document, sketch, photograph, photographic negative, plan, model, or knowledge, willfully and without proper authority, communicates or attempt to communicate the same to any person not entitled to receive it, or to whom the same ought not, in the interest of the national defense, be communicated at that time; or whoever, being lawfully entrusted with any such document, sketch, photograph, photographic negative, plan, model, or knowledge, willfully and in breach of his trust, so communicates or attempts to communicate the same, shall be

precursor to various important sections of the current Espionage Act, penalized the illegal stealing, gathering, and generic communicating of information from in and around military installations.[18] Moreover, section two of the statute imposed a harsher penalty on the passing of such information to a foreign government.[19] In the extensive list of types of actions punishable, "publishes" was not included.[20]

A few years later, just two days after the United States entered World War I, Congress began debating the next major piece of legislation dealing with the protection of national security information, the Espionage Act of 1917.[21] The DSA was included in the new Espionage

---

> fined not more than one thousand dollars, or imprisoned not more than one year, or both.
>
> SEC. 2. That whoever, having committed any offense defined in the preceding section, communicates or attempts to communicate to any foreign government, or to any agent or employee thereof, any document, sketch, photograph, photographic negative, plan, model, or knowledge so obtained, taken, or made, or so entrusted to him, shall be imprisoned not more than ten years.

Id. A small amount of discussion occurred as to these provisions, as the House Judiciary Committee report is five pages long. H.R. Rep. No. 1941, 61st Cong., 3d Sess. (1911). The House of Representatives debate covered less than two pages of the Congressional Record. 46 CONG. REC. 2029-30 (1911). The Senate's discussions of the provisions also lacked extensive scrutiny. *Id.* at 3516.

[18] 36 Stat. 1804 (1911). Of the little discussion in the House regarding the statute, House Judiciary Chairman Parker was asked about the meaning of the phrase "to which he is [not] entitled." 46 CONG. REC. 2030 (1911). Chairman Parker replied that the first draft of the statute included the word "wrongfully," but the Committee determined that not entitled was less ambiguous than wrongfully. *Id.* However, the Chairman did not specify as to how "not entitled" was any less vague than the previous language. Edgar & Schmidt, *supra* note 16, at 1003. Such sloppy language throughout the statute was adopted by subsequent legislation. *Id.* at 1005 (explaining that "the formless terms of the 1911 Act were accorded a respect and a putative clarity in later legislative stages out of all keeping with the casual process that spawned them").

[19] 36 Stat. 1804 (1911).

[20] Edgar & Schmidt, *supra* note 16, at 940.

[21] 40 Stat. 217 (1917) (current version included in 18 U.S.C. §§ 793-794 (2006)). The statutes, which have undergone little material alterations since their passage, have now been codified in 18 U.S.C. §§ 793(a)–(d) and § 794. In full §§ 793(a)–(d) state:

> (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, 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

Act, with the amendment that its prohibitions were criminal only when accompanied by "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."[22]

> 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 such 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; or
> (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 . . . shall be fined under this title or imprisoned not more than ten years, or both.

Id.

[22] 40 Stat. 217 (1917) (current version included in 18 U.S.C. §§ 793-794 (2006)). *See supra* note 21. The provisions extended the 1911 Act significantly, as they include prohibitions

As debate concerning the Act was ongoing, President Wilson's administration encouraged Congress to include in the Act a provision that would enable the prosecution of persons or entities that published any type of defense information.[23] The section was eventually defeated by close votes in both houses of Congress.[24] The only prohibition against publication that was passed is now included in 18 U.S.C. § 794(b), which mandates punishment for the publication of military information in a time of war with intent or reason to believe that the United States will be injured or a foreign nation will be aided.[25]

---

against those persons who possess both lawful and illegally-obtained national defense information. Edgar & Schmidt, *supra* note 16, at 1005-06.

[23] The proposal provided that:

> [d]uring any national emergency resulting from a war to which the United States is a party, or from threat of such a war, the President may, by proclamation, declare the existence of such emergency and, by proclamation, prohibit the publishing or communicating of, or the attempting to publish or communicate any information relating to the national defense which, in his judgment, is of such character that it is or might be useful to the enemy. Whoever violates any such prohibition shall be punished by a fine of not more than $10,000 or by imprisonment for not more than 10 years, or both: *Provided*, That nothing in this section shall be construed to limit or restrict any discussion, comment, or criticism of the acts or policies of the Government or its representatives or the publication of the same.

55 CONG. REC. 1763; *see also* Edgar & Schmidt, *supra* note 16, at 940.

[24] Edgar & Schmidt, *supra* note 16, at 956. The Senate defeated bill 8148 by a vote of 39 to 38, with 19 Senators choosing not to vote. *Id.* The bill would have prohibited, in wartime but without any culpability requirement, a person or entity from publishing or communicating a large range of defense information, including information regarding movement of armed forces, war materials, plans of military operations, "or any other information relating to the public defense or calculated to be, or which might be, useful to the enemy." N.Y. Times Co. v. United States, 403 U.S. 713 (1971); Edgar & Schmidt, *supra* note 16, at 947. Republican Senator Albert B. Cummins claimed that the act gave too much power to the executive branch. *Id.* He argued that "[u]nder this provision the President can absolutely command silence in the United States upon every subject mentioned . . . . He can suppress every suggestion concerning the national defense in every newspaper of the land." 54 CONG. REC. 3492 (1917); Edgar & Schmidt, *supra* note 16, at 947. A similar provision in the House bill was defeated by a vote of 221 to 167, with one answering "present" and 43 abstaining. Edgar & Schmidt, *supra* note 16, at 960-61.

[25] 18 U.S.C. § 794(b) provides:

> 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

In 1938, Congress passed three additional sections of the Espionage Statutes which dealt with photographing and military installations and subsequent publishing or sale of them.[26] These statutes, which are relatively straightforward, produced very little congressional debate, and few prosecutions have stemmed from them.[27]

One additional subsection of section 793, inserted in 1950, must be mentioned before a deeper discussion of the statutes' language can be examined.[28] Following World War II, Congress passed the Internal Security Act of 1950, which included section 793(e), prohibiting anyone who had unauthorized defense information from the willful communication of it to those persons or entities not entitled to receive it.[29] Additionally, Congress created an offense for the simple retention of such material.[30]

> 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.

Id.; *see also* Edgar & Schmidt, *supra* note 16, at 940-41. President Wilson's provision was defeated in part because Wilson's political opponents feared that it could be used to silence criticism of America's entrance into the World War I. *Id.* at 941. It was feared that any disapproval of foreign affairs could be muffled via the excuse that it was protecting national security secrets. *Id.*; *see also* Geoffrey R. Stone, *Judge Learned Hand and the Espionage Act of 1917: A Mystery Unraveled*, 70 U. CHI. L. REV. 335, 346-49 (2003) (discussing the heated debate over the "press censorship" provision).

26 18 U.S.C. §§ 795-97 (2006).

27 Edgar & Schmidt, *supra* note 16, at 1071.

28 *See infra* Part III.A.

29 18 U.S.C. § 793(e) (2006). In full, the statute reads:

> 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 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…[s]hall be fined under this title or imprisoned not more than ten years, or both.

Id.; *see also* Edgar & Schmidt, *supra* note 16, at 1022 (commenting "that for the third time in as many attempts, Congress had virtually no understanding of the language and effect of 793(d) and (e)").

30 18 U.S.C. § 793(e).

As mentioned earlier, phrases such as "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," "relating to the national defense," and "any person not entitled to receive it" are located throughout the Espionage Act.[31] Extensive scholarly writings have attempted to bring understanding to these ambiguous phrases, with little success.[32] Indeed, when two Columbia law professors, Harold Edgar and Benno C. Schmidt, Jr., analyzed the statutes in the 1970s, in what is perhaps the definitive examination of the provisions, they concluded that "the statutes implacably resist the effort to understand."[33]

The legislative history of sections 793 and 794 indicates that although Congress refused to pass President Wilson's broad press censorship proposal, it instead adopted these statutes, and in doing so did not intend to prohibit journalists from publishing defense information.[34] However, the plain language of the statutes themselves does not exclude the publication of defense information from their prohibitive reach.[35] Thus, although there continues to be uncertainty as to whether a journalist could be prosecuted under these statutes after publishing national security secrets, there does exist one other Federal Criminal Code provision that, after examining both its legislative history and its plain language, points towards the likely permittance of such prosecution.[36]

---

31 Such phrases are found in 18 U.S.C. §§ 793(a)–(e) and 794(a). For clarification purposes, throughout the rest of this Note, when "Espionage Act" is mentioned, it will refer only to 18 U.S.C. §§ 793–794.

32 *See, e.g.*, United States v. Rosen, 445 F. Supp. 2d 602, 613 (E.D. Va. 2006) (stating that the Act has been "criticized . . . as excessively complex, confusing, indeed impenetrable."); N.Y. Times Co. v. United States, 403 U.S. 713, 753 (1971) (Harlan, J., dissenting) (commenting that § 793(e) as a "singularly opaque statute"); Edgar & Schmidt, *supra* note 16, at 941-42 ("Unfortunately, the proponents of culpability requirements were more concerned with obtaining their inclusion than elucidating their meaning. Ambiguity pervades the Espionage Act . . . ."); Jereen Trudell, Note, *The Constitutionality of Section 793 of the Espionage Act and Its Application to Press Leaks*, 33 WAYNE L. REV. 205, 211 (1986) ("[I]t is impossible to determine exactly what Congress meant when it enacted the statute.").

33 Edgar & Schmidt, *supra* note 16, at 930.

34 *Id.* at 1057 ("Congress demonstrated by the narrowing and ultimate rejection of the Wilson Administration's broad proposed prohibition on publication of defense information that it did not intend to enact prohibitions on publication or communication motivated by the desire to engage in public debate or private discussion").

35 *Id.* at 937 ("[T]he language of the statutes has to be bent somewhat to exclude publishing national defense material from its [criminal] reach, and tortured to exclude from criminal sanction preparatory conduct necessarily involved in almost every conceivable publication" of military secrets).

36 *See infra* Part II.B.

B. The COMINT Statute

In 1950, Congress passed another provision to the Federal Criminal Code, codified as 18 U.S.C. § 798, which prohibited, among other things, the willful publishing of classified United States information related to communication intelligence.[37] In enacting this provision, Congress

---

[37] 18 U.S.C. § 798. The statute, titled "Disclosure of [C]lassified [I]nformation," provides:

> (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.
>
> (b) As used in this subsection (a) of this section –
>
> The term "classified information" means information which, at the time of a violation of this section, is, for reasons of national security, specifically designated by a United States Government Agency for limited or restricted dissemination or distribution;
>
> The terms "code," "cipher," and "cryptographic system" include in their meanings, in addition to their usual meanings, any method of secret writing and any mechanical or electrical device or method used for the purpose of disguising or concealing the contents, significance, or meanings of communications;
>
> 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;
>
> The term "communications intelligence" means all procedures and methods used in the interception of communications and the obtaining of information from such communications by other than the intended recipients;
>
> The term "unauthorized person" means any person who, or agency which, is not authorized to receive information of the categories set forth in subsection (a) of this section, by the President, or by the head of a department or agency of the United States Government which is

targeted a very narrow category of information that it deemed crucially important to be protected from our nation's enemies.[38] The provision, which has come be known as the COMINT statute, was enacted in direct response to a newspaper article published by the *Chicago Tribune* in the midst of World War II.[39] Shortly following America's victory over Japan at the battle of Midway, the *Tribune* ran a front-page article that disclosed the highly secretive information that the strength, nature, and even individual ship names of the approaching Japanese task forces were known to the United States commanders days prior to the engagement, with the reasonable conclusion that Japan's naval codes had been broken.[40] Since its exposure threatened to lengthen the war and thus lead to further military deaths, both the War Department and Justice Department encouraged a prosecution under the Espionage Act, and by August 1942, prosecutors had brought the issue before a federal grand jury.[41] However, the government subsequently decided to drop the charges to eliminate the risk of disseminating additional classified information to the jurors.[42] Even if charges had been brought to finality,

---

> expressly designated by the President to engage in communication intelligence activities for the United States.

Id.

[38] H.R. Rep. No. 81-1895, at 2 (1950). The House Judiciary Committee concluded that Section 798 "is an attempt to provide just such legislation for only a small category of classified matter, a category which is both vital and vulnerable to an almost unique degree." *Id.*

[39] Gabriel Schoenfeld, *Has the New York Times Violated the Espionage Act?*, COMMENTARY, Mar. 2006, at 24-25 (discussing possible statutes that could or could not be utilized against the *New York Times* for its disclosure of the classified NSA program). COMINT simply stands for communications intelligence, and:

> refers to those activities that produce intelligence by interception and processing of foreign communications passed by radio, wire, or other electromagnetic means . . . and by the processing of foreign encrypted communications, however transmitted. Interception comprises search, intercept, and direction-finding. Processing comprises range estimation, transmitter operator identification, signal analysis, traffic analysis, cryptanalysis, decryption, study of plaintext, the fusion of these processes, and the reporting of the results . . . .

DESMOND BALL, SIGNALS INTELLIGENCE IN THE POST-COLD WAR ERA 122 (1993) (quoting U.S. National Security Council Directive no. 6, 17 Feb. 1972).

[40] *See Navy Had Work of Jap Plan to Strike at Sea*, CHI. TRIBUNE, June 7, 1942, at A1. The critical information, attributed to "reliable sources in . . . naval intelligence," disclosed one of the outstanding breakthroughs of Allied forces in the war, which would surely continue to serve American war efforts to a great degree if Japan did not know that it had been broken and continued to use the same cryptographic system. Schoenfeld, *supra* note 39, at 24.

[41] Schoenfeld, *supra* note 39, at 25.

[42] *Id.* Additionally, the Japanese continued to use their same cryptographic system, JN-25, either because they never learned of the *Tribune* article, or persisted to believe that their

it is questionable whether the newspaper or its journalists would have been convicted under sections 793 or 794.[43]

Thus, in Congress' passage of section 798, it certainly had the *Tribune* incident in mind when it directed criminal sanctions at disclosures of sensitive communications intelligence.[44] Indeed, Congress twice had refused to adopt a measure that would have made a person's unauthorized disclosure of any classified information subject to criminal prosecution.[45] Therefore, the COMINT statute was drafted especially with the rationale of balancing public debate and the necessary security of national defense material and information.[46]

Moreover, the COMINT statute as written and enacted was a "model of precise draftsmanship."[47] As the provision unambiguously asserts via its explicit use of the word "publishes," section 798 is a proscription upon public speech that is directly aimed at preventing newspapers, magazines, and similar media from making known certain communications intelligence.[48] Additionally, the law's mens rea requirement is met upon knowingly and willfully accomplishing the forbidden disclosure, without any additional condition that the information be used to injure the United States or aid a foreign country.[49] Moreover, Congress dodged additional potential application difficulties by declining to include any prerequisite that America be at war.[50]

Perhaps indicating the overwhelming support of the statute, and in light of the recent *Chicago Tribune* article and the deliberate contraction to

---

codes were unbreakable. *Id.* at 24-25; *see generally* DAVID KAHN, THE CODEBREAKERS (1967) (explaining the history of secret communications, including the Japanese in World War II).

43 *See infra* Part III.A.

44 Schoenfeld, *supra* note 39, at 28.

45 Edgar & Schmidt, *supra* note 16, at 1056. *See* REPORT OF THE JOINT COMMITTEE OF THE INVESTIGATION OF THE PEARL HARBOR ATTACK, S. Doc. No. 79-244 (1946); S. 1019, 80th Cong. (1950); S. 2680, 80th Cong. (1950). The proposals would have criminalized the "revelation or publication, not only of direct information about United States codes and ciphers themselves but of information transmitted in United States codes and ciphers." Edgar & Schmidt, *supra* note 16, at 1068. Such provisions would have prohibited publication regarding a large amount of military and diplomatic dispatches and information sent by the government via codes and ciphers both internationally and intranationally. *Id.*

46 Schoenfeld, *supra* note 39, at 28.

47 Edgar & Schmidt, *supra* note 16, at 1065.

48 *Id.*; *see also* Schoenfeld, *supra* note 39, at 28.

49 Edgar & Schmidt, *supra* note 16, at 1065.

50 Schoenfeld, *supra* note 39, at 28; *see also* Michael D. Ramsey, *Presidential Declarations of War*, 37 U.C. DAVIS L. REV. 321 (2003) (discussing the evolution of the official declaration of war in the United States).

the narrow amount of information prohibited by the statute, the House of Representatives passed section 798 without substantive debate.[51] Moreover, the Senate conducted very little discussion prior to passing it, as well.[52] As Edgar and Schmidt have pointed out, the provision had been drafted "with concern for public speech having been thus respected," and had even been supported by the American Society of Newspaper Editors.[53]

C. The Pentagon Papers: Watering the Seeds of Prosecution

Perhaps the most famous Supreme Court case concerning the balance of the right to know and the need to withhold is *New York Times Co. v. United States*.[54] The thrust of the case was an attempt by the government to receive injunctive relief against the *New York Times* and the *Washington Post* in order to prohibit them from continuing to publish the contents of the classified and highly secretive Pentagon Papers.[55] In a *per curiam* decision, the Court determined that the government failed to meet the heavy burden required to justify the imposition of a prior restraint against the newspapers.[56] However, the nine individual opinions that followed indicated a splintered Court regarding the Justices' reasoning, dicta, and policy concerns.[57]

---

51 96 CONG. REC. 6082 (1950).

52 95 CONG. REC. 2774 (1949).

53 Edgar & Schmidt, *supra* note 16, at 1069. In one of history's ironic twists, the main editors of the *New York Times* were active members of the American Society of Newspaper Editors. Schoenfeld, *supra* note 39, at 28.

54 N.Y. Times Co. v. United States, 403 U.S. 713 (1971). The litigation has come to be known as the Pentagon Papers case, named after the Defense Department study detailing American involvement in Vietnam. *Id.* at 714. The study, commissioned by Secretary of Defense Robert McNamara, was officially titled "History of U.S. Decision-Making Process on Vietnam Policy." *Id.* A federal district court in New York refused to issue the injunction requested by the government to stop the publishing of sections of the study in the *Times*. United States v. N.Y. Times Co., 328 F. Supp 324 (S.D.N.Y. 1971). However, the Second Circuit Court of Appeals reversed and approved the injunction. United States v. N.Y. Times Co., 444 F.2d 544 (2nd Cir. 1971).

55 *N.Y. Times Co.*, 403 U.S. 713. Importantly, the Government argued only for an injunction, and its brief lacked any mention of the espionage statutes, presumably because no section authorizes injunctive, but rather only criminal, relief. *See also* Edgar & Schmidt, *supra* note 16, at 931.

56 *Id.* at 714.

57 *Id.* at 713. Justice Black and Justice Douglas each wrote a concurring opinion, while joining each other. The same can be said for Justices Stewart and White. Justice Brennan authored a concurring opinion, as did Justice Marshall. Justice Harlan wrote the principal dissent, which was also joined by Chief Justice Burger and Justice Blackmun. Finally, Chief Justice Burger and Justice Blackmun each wrote a separate dissenting opinion.

A brief examination of the differing opinions denotes the fractured nature of the Justices' rationales.[58] Justices Black and Douglas indicated that they believed the First Amendment is an absolute, in that no governmental restraints can be placed on the press' right to publish any and all information.[59] While Justice Brennan's concurrence did not go to such an extreme, he did assert that the First Amendment bars the judiciary from stopping the publication of material that a newspaper already has in its possession.[60]

More pertinent to the issue of this Note were the opinions of the remaining six Justices. First, Justice Stewart, while concurring that the injunction should not be granted, did concede that Congress has the power and ability to pass criminal laws to protect secret government information.[61] Although he did not specifically name section 798, Justice Stewart stated that "Congress has passed such laws, and several of them are of very colorable relevance" to the case at hand.[62] Moreover, Justice White expended a substantial portion of his opinion to further elaborate upon possible criminal prosecutions.[63] Explicitly referring to section 798 as a provision of the Criminal Code that would allow prosecutions against publishers, Justice White noted that he would not hesitate to sustain a conviction if the elements of the statute were met.[64]

Justice Marshall, while maintaining that there may have been a criminal statute that fit the facts of the Pentagon Papers situation, commented that various provisions did in fact criminalize the dissemination of certain government secrets.[65] Yet, through his

---

58 *See infra* notes 59-68 and accompanying text.

59 *N.Y. Times Co.*, 403 U.S. at 714-15 (Black, J., concurring); *see id.* at 720 (Douglas, J., concurring).

60 *Id.* at 725 (Brennan, J., concurring).

61 *Id.* at 730 (Stewart, J., concurring).

62 *Id.* Justice Stewart went on to assert that, if the government decided to proceed with criminal sanctions under the appropriate statutes, it would be the duty of the judicial branch to enforce them if constitutional. *Id.*

63 *Id.* at 733-40 (White, J., concurring).

64 *Id.* at 735. Justice White stated, "I would have no difficulty in sustaining convictions under these sections on facts that would not justify the intervention of equity and the imposition of a prior restraint." *Id.* at 737. Another section that Justice White pointed to for possible prosecution in this situation was 18 U.S.C. § 793(e). *Id.* at 737-40; *cf.* 403 U.S. at 745 (Marshall, J., concurring); *infra* note 65 (discussing the powers of the legislature to create laws that prohibited the disclosures of some classified government secrets).

65 *N.Y. Times Co.*, 403 U.S. at 743-45 (Marshall, J., concurring).

> Congress has on several occasions given extensive consideration to the problem of protecting the military and strategic secrets of the United States. This consideration has resulted in the enactment of statutes making it a crime to receive, disclose, communicate, withhold, and

observations concerning several other similar statutes, Justice Marshall made clear that it is the province of the legislature to criminalize certain disclosures, and the courts have the ultimate responsibility to enforce them.[66]

Furthermore, the three dissenters from the *per curiam* opinion also shed additional light on the issue of whether criminal sanctions were possible in situations where national defense information is published. Indeed, Chief Justice Burger explicitly approved of the notions of Justice White's concurrence regarding the application of criminal punishment.[67] Although the remaining two dissenters, Justices Harlan and Blackmun, did not overtly assert that criminal statutes existed which could be employed against the publishers, they did not explicitly disapprove of this view, as they would have granted the injunction against publishing the Pentagon Papers altogether.[68]

Heeding the guidance of these Supreme Court Justices, the government soon thereafter brought a fifteen-count indictment against the *New York Times* reporters who compiled and published the Pentagon Papers, Daniel Ellsberg and Anthony Russo.[69] The indictment charged

---

> publish certain documents, photographs, instruments, appliances, and information. The bulk of these statutes is found in chapter 37 of U. S. C., Title 18, entitled Espionage and Censorship.

Id. at 743.

66 *Id.* at 743-47. Justice Marshall also referenced previous attempts ultimately defeated by Congress that would have prohibited publishing certain government secrets. *Id.* at 746-47; *see also supra* notes 23-24 (describing President Wilson's broad censorship proposal that was eventually defeated by Congress). In 1957, the United States Commission on Government Security proposed an ultimately-defeated provision to Congress, stating that Congress should "enact legislation making it a crime for any person willfully to disclose without proper authorization, for any purpose whatever, information classified 'secret' or 'top secret,' knowing, or having reasonable grounds to believe, such information to have been so classified." *N.Y. Times Co.*, 403 U.S. at 747 (quoting the Report of Commission of Government Security, 619-20 (1957)).

67 *N.Y. Times Co.*, 403 U.S. at 748, 752 (Burger, C.J., dissenting) (stating "I should add that I am in general agreement with much of what Mr. Justice White has expressed with respect to penal sanctions concerning communication or retention of documents or information relating to the national defense").

68 *Id.* at 753-59 (Harlan, J., dissenting); *Id.* at 759-63 (Blackmun, J., dissenting).

69 Melville B. Nimmer, *National Security v. Free Speech: The Issues Left Undecided in the Ellsberg Case*, 26 STAN. L. REV. 311 (1974). Ellsberg, who was a member of the Defense Department commission that researched and authored the Pentagon Papers, was in possession of the Papers between August 1969 and May 1970. *Id.* at 312. During this time period, Ellsberg admittedly took them from his top secret safe and copied them at a location ten miles away. *Id.* at 313. Russo also admitted to helping Ellsberg achieve this task. *Id.*

the defendants with a violation of 18 U.S.C. §§ 793(d)-(e)[70] and 18 U.S.C. § 641.[71] However, all charges were dismissed against Ellsberg and Russo when Judge William Matthew Byrne, Jr., granted the defendants' motion to dismiss due to government misconduct.[72] As a result of this limited victory for Ellsberg and Russo, the merits of the case were never resolved, leaving commentators to ponder the hypothetical implications.[73]

While the Pentagon Papers case only tangentially affects possible prosecutions under the COMINT statute, it points toward the possibility of the prosecution of journalists for their publication of certain classified information.[74] Moreover, following the dismissal of the Ellsberg case for reasons other than the merits of the case, "[t]he specter of Ellsberg hangs over government officials, newsmen, and others who may in the future wish to disclose to the public vital governmental documents."[75] In the decades since these cases, few cases have considered the issue, but those that have are indicative of the judicial trend toward protection of national security.[76]

D. Tightening the National Security Screws

Throughout the 1970s and into the 1980s, as both foreign and domestic United States policy was influenced by the Cold War and nuclear proliferation, the necessity of government secrecy increased, as

---

70 See *supra* notes 21 and 29 for the full text of the provisions.

71 18 U.S.C. § 641 (2006). This provision criminalizes, among other things, the stealing, converting, and embezzling of government documents, which in this case included the Pentagon Papers. Nimmer, *supra* note 69, at 315. The application of this statute is outside the scope of this Note.

72 Ellsberg v. Mitchell, 353 F. Supp. 515, 516 n.1 (D.D.C. 1973) (citing United States v. Russo, No. 9373-(WMB)-CD (filed Dec. 29, 1971), *dismissed* (C.D. Cal. May 11, 1973)). The court granted the motion to dismiss due to "the totality of government misconduct, including the suppression of evidence, the invasion of the physician-patient relationship, the illegal wiretapping, the destruction of relevant documents and disobedience to judicial orders." Nimmer, *supra* note 69, at 311. Judge Byrne implemented this language in his oral grounds for dismissal, which coincided with the language of the defendants' oral motion to dismiss. *Id.* at 311 n.2.

73 *See, e.g.*, Nimmer, *supra* note 69 (discussing the possible outcome of the Ellsberg and Russo prosecution had the case been judged on its merits, concluding that they would have been found not guilty under 18 U.S.C. § 641, and that 18 U.S.C. §§ 793(d)–(e) would have been found unconstitutional due to facial overbreadth).

74 *See supra* notes 61-68 and accompanying text.

75 Nimmer, *supra* note 69, at 312.

76 *See infra* Part II.D.

both classic spies and leaks to the press became a serious problem.[77] Such media related activity and, in at least one case, subsequent prosecution, was evident in *United States v. Morison*.[78] In *Morison*, the government brought charges against Samuel Morison for violating sections 793 (d) and (e) of the Espionage Act after he provided classified photographs of a Soviet aircraft carrier to a British magazine, which were taken by a secret reconnaissance satellite.[79] When the District Court of Maryland convicted Morison under sections 793(d) and (e), it was the first time a court determined that the Espionage Act could be successfully applied to the act of providing documents or information to a member of the media, as opposed to an agent of a foreign government.[80]

On appeal, Morison argued that the provisions did not apply to this situation, because prosecutions under the Espionage Act had never been used against a person in his position.[81] However, the Fourth Circuit Court of Appeals agreed with the government that the literal words of the statutes did not prohibit such a conviction.[82] Importantly, the court expressly stated that simply because prosecutions under a provision are infrequent, it does not follow that the statutory language should be invalidated.[83] As a result, the court affirmed the district court's conviction of a two-year prison term.[84]

---

77 *See* Thomas S. Martin, *National Security and the First Amendment: A Change in Perspective*, 68 A.B.A. J. 680 (1982). Martin, a deputy assistant attorney general in the Civil Division of the Department of Justice during the Carter administration, stated that a large portion of disclosures came not from spies but from authors and journalists who made previously-classified information public through media outlets. *Id.* at 680-81. This was because "[t]hey were idealists convinced that the world would be a better place if particular secret information were available to the public. They were journalists who took from Vietnam and Watergate the proposition that disclosure of government secrets is inherently a public service and even a primary responsibility of the profession." *Id.* at 681.

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

79 *Id.* at 1060-61. Morison, a former civilian analyst at the Naval Intelligence Support Center ("NISC") in Suitland, Maryland, had been employed from 1974 until October 1984. *Id.* at 1060. Additionally, he worked as a part-time editor of the British magazine *Jane's Fighting Ships*. *Id.* Due to his dissatisfaction at the NISC and in an attempt to gain a promotion with the magazine, Morison passed along three classified photographs of the Soviet carrier to the editor-in-chief of *Jane's Fighting Ships*, Derek Wood. *Id.* at 1060-61.

80 604 F. Supp. 655 (Md. 1985); *see also* David H. Topol, United States v. Morison*: A Threat to the First Amendment Right to Publish National Security Information*, 43 S.C. L. REV. 581, 590 (1992) (arguing that *Morison* set an alarming precedent by interpreting sections 793(d) and (e) to allow media-related prosecutions, as opposed to classic spy situations).

81 *Morison*, 844 F.2d at 1063.

82 *Id.* at 1067.

83 *Id.* at 1067.

Additionally, a case is currently being litigated that has a bearing on the constant balance between national security and press leaks.[85] *United States v. Rosen*[86] involves the actions of two officials of the American Israel Public Affairs Committee ("AIPAC"), a Washington, D.C. lobbyist group.[87] The AIPAC officials, Steven Rosen and Keith Weissman, were accused of receiving classified information from Lawrence Franklin, an employee of the Defense Department, and then conspiring to transfer the information to an Israeli diplomat and members of the media.[88] Rosen and Weissman were both charged with violating sections 793(e) and (g), while Rosen was additionally charged with violating section 793(d).[89]

> [T]he rarity of prosecution under the statutes does not indicate that the statutes were not to be enforced as written. We think in any event that the rarity of the use of the statute as a basis for prosecution is at best questionable for nullifying the clear language of the statute, and we think the revision of 1950 and its reenactment of section 793(d) demonstrate that Congress did not consider such statute meaningless or intend that the statute and its prohibitions were to be abandoned.

Id.

84 Schoenfeld, *supra* note 39, at 25. The court also determined that the statutes met other constitutional hurdles, such as the vagueness and overbreadth doctrines. *Id.* Over a decade after his release from prison, Morison received a full pardon in 2001 from President Clinton on his last day in office. *Id.* at 25 n.5.

85 *Id.* at 25.

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

87 *Id.* AIPAC has been described as one of the "most influential lobbying organizations" in Washington, one which lobbied on issues relating to American foreign policy in the Middle East. Dan Eggen & Jerry Markon, *2 Senior AIPAC Employees Ousted*, WASH. TIMES, Apr. 21, 2005, at A08.

88 *Rosen*, 445 F. Supp. 2d at 608-09. Franklin was a mid-level worker on the Iran desk in the Office of the Secretary of the Department of Defense, who held a top secret security clearance during the alleged illegal actions. *Id.* Following an alleged conspiracy by disclosing information to Rosen and Weissman beginning in late 2002, Franklin began to cooperate with the FBI in July of 2004. *Id.* at 608-10.

> On October 5, 2005, Franklin pled guilty to one count of conspiracy to communicate national defensey information to one not entitled to receive it, in violation of 18 U.S.C. §§ 793(d) and (g), and to one count of conspiracy to communicate classified information to an agent of a foreign government in violation of 50 U.S.C. § 783 and 18 U.S.C. § 371.

Id. at 608 n.3. Franklin was sentenced to a prison term of twelve-and-a-half years, which will be reviewed following the trial of Rosen and Weissman. Schoenfeld, *supra* note 39, at 25-26.

89 *Rosen*, 445 F. Supp. 2d at 610. Their indictment maintains that they used "their contacts within the U.S. government and elsewhere to gather sensitive U.S. government information, including classified information relating to national defense, for subsequent unlawful communication, delivery, and transmission to persons not entitled to receive it." Schoenfeld, *supra* note 39, at 25. Rosen's additional charge was based on his alleged aiding and abetting Franklin's transmission of a fax of classified document. *Rosen*, 445 F. Supp. 2d at 610.

In August of 2006, a district court in Virginia convicted Rosen and Weissman of all charges.[90] Despite the defendants' challenges of as-applied vagueness, facial overbreadth, and transgression of their First Amendment rights to free speech and to petition the government, the court asserted that the plain language of the provisions applied to classified information that had been "leaked" to them.[91]

The court discounted the defendants' assertion that because section 793(e) had never been applied to prosecute persons in their situation, it thus violated the fair warning element of the vagueness doctrine.[92] Rosen and Weissman, as non-government persons, argued that the intent of the statute was not to punish disseminators of already leaked information, thus the prosecution was "novel and unprecedented."[93] However, the court decided that the plain language of the statute prevailed under these circumstances, regardless of the fact that the defendants were non-government personnel.[94]

The AIPAC case is instructive because it highlights the issue of national security secrecy. First, Rosen and Weissman were not government employees, and thus *Rosen* stands, at least in part, for the proposition that the Espionage Act can be successfully applied to persons to whom information is leaked in the first place.[95] Moreover, the district court determined that the language of the statutes was sufficiently clear to pass constitutional scrutiny and was not overbroad.[96]

---

90 *Rosen*, 445 F. Supp. 2d at 645.

91 *Id.* at 628.

92 *Id.* at 627-28.

93 *Id.* The court emphasized that "labeling an event a 'leak' does not remove the event from the statute's scope. At best, the term 'leak' is a euphemism used to imply or suggest to a careless reader that the transmission of the information was somehow authorized. . . . [D]efendants frequent use of 'leak' as a characterization of what occurred is unavailing." *Id.* at 628-29.

94 *Id.* at 628. The court reasoned that "[i]n amending the statute in 1950, Congress made it quite clear that the statute was intended to apply to the transmission of national defense information by non-government employees by adding subsection (e)." *Id.* at 628 n.38.

95 Schoenfeld, *supra* note 39, at 26. There was not a violation of due process, as the defendants had argued, claiming that this prosecution was a "novel construction of a criminal statute . . . that neither the statute nor any prior judicial decision has fairly disclosed to be within its scope." *Rosen*, 445 F. Supp. 2d at 627. The defendants also asserted that they did not have fair warning that the statute applied to them, but the *Morison* decision had also considered the same argument and rejected it there as well. *Id.* at 628; *see also* United States v. Morison, 844 F.2d 1057, 1067 (4th Cir. 1988) (quoting United States v. Lanier, 520 U.S. 259, 266 (1997)).

96 *Rosen*, 445 F. Supp. 2d at 643; *but see District Court Holds That Recipients of Government Leaks Who Disclose Information "Related to the National Defense" May Be Prosecuted Under the Espionage Act*, 120 HARV. L. REV. 821, 823-24 (2007) (asserting that the Rosen decision was

Finally, the indictment and subsequent conviction of Rosen and Weissman indicate that it is illegal both to gain possession of classified information and subsequently forward it to others, including a "member of the media."[97] However, what if Rosen and Weissman, as opposed to passing along the information secretly, had instead written an article and published it on the front page of a major national newspaper?

E. The New York Times *and its Disclosures*

Within the past several years, the *New York Times* has published prominent articles that have disclosed two classified anti-terrorist programs that were illegally leaked to it from anonymous sources inside the United States' government.[98] First, on December 16, 2005, the *New York Times* published a front-page article under the headline "Bush Lets U.S. Spy on Callers Without Courts."[99] The article, written by journalists James Risen and Eric Lichtblau, described the existence of a highly classified terrorist surveillance program conducted by the National Security Agency ("NSA") and the manner in which it operated.[100] Second, Lichtblau and Risen authored another article, published in the *New York Times* on June 23, 2006, titled "Bank Data Sifted in Secret by U.S. to Block Terror," which disclosed the manner in which the government tracks the finances of suspected terrorists.[101]

---

incorrect, as the Espionage Act is unconstitutionally vague as applied to situations where the First Amendment is implicated); *see also* Edgar & Schmidt, *supra* note 16 and accompanying text.

97 *Rosen*, 445 F. Supp. 2d at 626 (asserting that even if such a transmission of information relating to the national defense to the media was in his mind "an act of patriotism," he could still be convicted of willfully disclosing the information); *see also* Schoenfeld, *supra* note 39, at 26.

98 *See infra* notes 99, 101.

99 James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES, Dec. 16, 2005, at A1. The article was a precursor to Risen's impending publication of a book detailing at length, among other intelligence matters, the NSA program that was the subject of the *Times'* article. *See generally* JAMES RISEN, STATE OF WAR (2006).

100 Risen & Lichtblau, *supra* note 99.

101 Eric Lichblau & James Risen, *Bank Data Sifted in Secret by U.S. to Block Terror*, N.Y. TIMES, June 23, 2006, at A1. Barclay Walsh also contributed to the article. *Id.* Similar articles were published the same day in two other major American newspapers, the *Los Angeles Times* and the *Wall Street Journal*. *See* Josh Meyer & Greg Miller, *Secret U.S. Program Tracks Global Bank Transfers*, L.A. TIMES, June 23, 2006, at A1; Glenn R. Simpson, *Treasury Tracks Financial Data in Search Effort*, WALL ST. JOURNAL, June 23, 2006, at A1; Editorial, *Fit and Unfit to Print*, WALL ST. JOURNAL, June 30, 2006, *available at* http://www.opinionjournal.com/editorial/feature.html?id=110008585 (explaining that because government officials had not told the *Wall Street Journal* that it had urged the *New York Times* not to publish the story, the *Journal* went forth with publication).

Relying on numerous anonymous government officials, the December 2005 article disclosed that the NSA program, authorized by a 2002 presidential order, allowed the NSA to monitor international telephone and e-mail communications between people inside the country and suspected terrorist-related persons outside the United States.[102] The program allowed the NSA to monitor such communications without applying for warrants from the Foreign Intelligence Security Act ("FISA") courts, the 1978 legislation that had previously authorized such surveillance.[103] The government has argued that Congress empowered the President to create the program when it enacted the Authorization for Use of Military Force ("AUMF") shortly after the terrorist attacks of September 11, 2001.[104] The NSA program has been praised by the administration and its supporters as one of the most crucial anti-terrorism weapons employed by the United States since the

---

[102] Risen & Lichtblau, *supra* note 99, at A1 ("[n]early a dozen current and former officials, who were granted anonymity because of the classified nature of the program, discussed it with reporters for The *New York Times* because of their concerns about the operation's legality and oversight"). At least one of the anonymous sources has been reported as Russell Tice, a former longtime employee of the NSA. Brian Ross, *NSA Whistleblower Alleges Illegal Spying* (Jan. 10, 2006), *available at* http://abcnews.go.com/WNT/Investigation/story?id=1491889.

[103] Risen & Lichtblau, *supra* note 99. The constitutionality of the program has been greatly questioned, especially by politicians, civil libertarians, and interest groups. Schoenfeld, *supra* note 39, at 23; *see, e.g.*, *Washington in Brief* (Feb. 14, 2006), http://www.washingtonpost.com/wpdyn/content/article/2006/02/13/AR2006021302006.html (last visited Oct. 12, 2006) (discussing the fact that the American Bar Association had denounced the program as unconstitutional); *see also* CNN, *Bush: Secret Wiretaps Have Disrupted Potential Attacks* (Dec. 20, 2005), http://www.cnn.com/2005/POLITICS/12/19/nsa/index.html (last visited Oct. 12, 2006) ("'This administration is playing fast and loose with the law in national security. The issue here is whether the president of the United States is putting himself above the law, and I believe he has done so.'") (quoting Wisconsin Democratic Senator Russ Feingold). Following the article's publishing, President Bush declared that he did instruct the NSA to "intercept the international communications of people with known links to al Qaeda and related terrorist organizations[,]" but that before such surveillance, "the government must have information that establishes a clear link to these terrorist networks." The White House, President's Radio Address, http://www.whitehouse.gov/news/releases/2005/12/print/20051217.html (last visited Oct. 12, 2006).

[104] The AUMF states:

> [t]hat the President is authorized to use all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided the terrorist attacks that occurred on September 11, 2001, or harbored such organizations or persons, in order to prevent any future acts of international terrorism against the United States by such nations, organizations or persons.

Pub. L. No. 107-40, § 2(a), 115 Stat. 224 (Sept. 18, 2001).

attacks of September 11th to disrupt and thwart future plots.[105] Several government officials have publicly proclaimed that the program was a central tool in fighting terror.[106] The importance of the secrecy of the program was highlighted by the fact that Bush administration officials pleaded with the *Times* not to publish the details of the classified program.[107]

In August of 2006, a federal district court held the program unconstitutional as a violation of the First and Fourth Amendments, in addition to the separation of powers doctrine.[108] On appeal, however, on

---

[105] Risen & Lichtblau, *supra* note 99, at A1. Although the extent to which the NSA program has been successful is still unknown, it has been credited with discovering the plot of terrorist Iyman Faris, the American citizen who pled guilty in 2003 to plotting to topple the Brooklyn Bridge with blowtorches. *Id.* Additionally, an al Qaeda plan to employ fertilizer bomb attacks on British bars and train stations was uncovered in 2004 partly from information gathered through the NSA program. *Id.*; *see also, e.g.,* Pierre Thomas, Mary Walsh & Jason Ryan, *Officials Search for Terrorist Next Door* (Sept. 8, 2003), *available at* http://abcnews.go.com/WNT/story?id=129090&page.

[106] Gabriel Schoenfeld, Statement Before the Senate Committee on the Judiciary (June 6, 2006), *available at* http://www.fas.org/irp/congress/2006_hr/060606schoenfeld.pdf#search=%22edgar%20schmidt%20bent%20tortured%20sanction%22. The National Intelligence Director, John Negroponte, has described the NSA program as "crucial for protecting the nation against its most menacing threat." *Id.* "FBI director Robert Mueller has [stated that the program] has 'been valuable in identifying would-be terrorists in the United States.'" *Id.* Former director of the NSA and current Director of the Central Intelligence Agency, General Michael Hayden, asserted that it was his "professional judgment that if we had had this program in place [before 9/11], we would have identified some of the al-Qaeda operatives in the United States." *Id.* Porter Goss, former Director of the Central Intelligence Agency and predecessor of General Hayden, referred to the disclosure of the NSA program as having caused "very severe" damage to United States' intelligence collection capabilities. *Id.* Jane Harman, the ranking Democratic member of the House Intelligence Committee, maintained "that the disclosure of the NSA program 'damaged critical intelligence capabilities.'" *Id.*

[107] Risen & Lichtblau, *supra* note 99, at A1. The *Times* decided to delay publication for over a year after it first met with administration officials to conduct more investigation. *Id.*; *see also* Schoenfeld, *supra* note 39, at 24.

[108] Am. Civil Liberties Union v. Nat'l Sec. Agency/Cent. Sec. Serv., 438 F. Supp. 2d 754 (E.D. Mich. 2006). The court found that because the wiretaps were not implemented in accordance with FISA, the "program . . . [is] obviously in violation of the Fourth Amendment." *Id.* at 775. Additionally, the court reasoned that because of the nature of the chilling effect the wiretaps had on the speech of the plaintiffs, their First Amendment rights were also violated. *Id.* at 776. Finally, the court asserted that because the Congress enacted FISA, and the President violated its provisions, the Separation of Powers doctrine was infringed. *Id.* at 779; *see also* Fletcher N. Baldwin, Jr. & Robert B. Shaw, *Down to the Wire: Assessing the Constitutionally of the National Security Agency's Warrantless Wiretapping Program: Exit the Rule of Law*, 17 U. FLA. J.L. & PUB. POL'Y 429 (2006) (claiming that the program cannot withstand legitimate constitutional scrutiny). The ruling was subsequently appealed by the government to the Sixth Circuit Court of Appeals, which granted the government's request to delay the application of the injunction. Am. Civil Liberties Union v. Nat'l Sec. Agency/Cent. Sec. Serv., 467 F.3d 590 (6th Cir. 2006).

July 6, 2007, the Sixth Circuit Court of Appeals vacated the district court's order and dismissed the action because the plaintiffs lacked standing for their claims.[109] The court held that the plaintiffs, which included lawyers, academics, and journalists who often had contact with people who they believed were targets of the NSA program, failed to meet the standing requirement under any of their six claims.[110]

However, after the district court's determination of the program's illegality, but before the Sixth Circuit reversed that decision, in January of 2007, the Bush administration decided not to reauthorize the NSA program.[111] Attorney General Alberto Gonzales sent a letter to the Senate Judiciary Committee in which he maintained that all government electronic surveillance will be first endorsed by the FISA courts.[112] While Gonzales claimed that court orders by a judge of the FISA court will allow for sufficiently quick responses to administration requests for warrants, some in the media questioned why the Bush administration seemingly altered its position on the issue.[113]

Nearly six months after the NSA disclosure, the *Times* once again published an article describing another top secret program, commonly known as the Terrorist Finance Tracking Program ("TFTP").[114] A

---

[109] Am. Civil Liberties Union v. Nat'l Sec. Agency, 493 F.3d 644, 687-88 (6th Cir. 2007) (the majority was written by Circuit Judge Alice M. Batchelder, with a concurring opinion by Judge Julia Smith Gibbons, and Circuit Judge Ronald Lee Gilman dissenting).

[110] *Id.* at 659-83. The claims asserted by the plaintiffs included a First Amendment free speech challenge, a Fourth Amendment privacy challenge, a separation of powers challenge, a review under the Administrative Procedure Act, a challenge under Title III of the Omnibus Crime Control and Safe Streets Act, and a challenge under FISA. *Id.*

[111] Prepared Opening Remarks of Attorney General Alberto R. Gonzales, *Justice Department Oversight Hearing of the Senate Judiciary Committee* (Jan. 18, 2007).

[112] *Id.* In particular, Gonzales asserted that "surveillance into or out of the United States where there is probable cause to believe that one of the communicants is a member or agent of al Qaeda or an associated terrorist organization [will be] subject to the approval of the FISA Court." *Id.*

[113] *See, e.g.*, Rob Hendin, *Why Warrantless Wiretapping Is No More* (Jan. 19, 2007), *available at* http://www.cbsnews.com/stories/2007/01/19/politics/main2376652.shtml; Andrew C. McCarthy, *The ACLU Loses in Court*, THE WEEKLY STANDARD, July 23, 2007, at 17-18 (explaining that because FISA requires a probable cause standard to be met before surveillance of a foreign person may occur, and the Fourth Amendment authorizes searches when the much less stringent standard of reasonableness is met, FISA does not allow surveillance on everyone the nation needs to monitor during this war); David B. Rivkin & Lee A. Casey, *Surveillance Showdown* (Sept. 30, 2007), *available at* http://www.opinionjournal.com/forms/printThis.html?id=110010670 (questioning whether "any sane country [would] purposefully limit its ability to spy on enemy communications in time of war," concluding that "for the first time in history, the U.S. is asked to collect less intelligence about the enemy while prosecuting a war.")

[114] Lichblau & Risen, *supra* note 101.

Treasury Department program operated in conjunction with the CIA, the TFTP monitors a network of worldwide financial institutions without the knowledge of many banks or their customers.[115]

In contrast to the NSA program, there have been few concrete objections to the TFTP claiming that it is an unconstitutional program, other than a supposed lack of oversight.[116] This is because SWIFT is required to give this information to nations under a 1977 statute, the International Emergency Economic Powers Act ("IEEPA"), when subpoenaed by governments pursuant to a Presidential declaration of national emergency.[117]

Accordingly, there has been a large amount of critical response to the decision by the *Times* to publish both the Risen and Lichtblau articles.[118] Foremost, President Bush labeled the disclosure of the NSA program as a "shameful act."[119] Moreover, the President has indicated his concern that the disclosures will cause targets of the program to change their

---

[115] Meyer & Miller, *supra* note 101, at 1. The major conglomeration that allowed the U.S. to monitor their records is formally known as the Society for Worldwide Interbank Financial Telecommunication, or SWIFT. Lichtblau & Risen, *supra* note 101, at A1. SWIFT operates when banks from all around the globe issue international, often overseas, completed monetary transfers, but does not provide information regarding individual bank account information. Stuart Levey, *Under Secretary Terrorism and Financial Intelligence, Testimony Before the House Financial Services Subcommittee on Oversight and Investigations* (July 11, 2006), at 1, http://www.treas.gov/press/releases/hp05.htm (last visited Nov. 14, 2006). Additionally, SWIFT contains no information about most normal domestic transactions in the United States, such as ATM withdrawals, checks, or deposits. *Id.* at 2.

[116] Meyer & Miller, *supra* note 101, at 2. "Critics complain that these efforts are not subject to independent governmental reviews designed to prevent abuse, and charge that they collide with privacy and consumer protection laws in the United States." *Id.*

[117] Levey, *supra* note 115, at 2. In response to the terrorist attacks of September 11, 2001, President Bush soon thereafter issued Executive Order 13224, which is the basis for the required subpoenas. *Id.* The Order is renewed yearly as the terrorist threat has continued. *Id.*

[118] *See infra* notes 119-24 and accompanying text.

[119] NBC News and News Services, *Bush Says Leaking Spy Program a 'Shameful Act'* (Dec. 20, 2005), http://www.msnbc.msn.com/id/10530417/ (last visited Oct. 12, 2006). Bush promised to continue to employ the NSA program "for so long as the nation faces the continuing threat of an enemy that wants to kill American citizens." *Id.* The American Society of Newspapers Editors issued a news release that supported the actions of the *Times*, stating in part that "[t]he administration of President George W. Bush and some members of Congress are threatening America's bedrock values of free speech and free press with their attempts to demonize newspapers for fulfilling their constitutional roles in our democratic society." American Society of Newspapers Editors, *ASNE Criticizes President, Lawmakers for Attacks on Newspapers* (June 30, 2006), http://www.asne.org/index.cfm?ID=6346 (last visited Jan. 11, 2006).

tactics.[120] In the weeks following the disclosure of the NSA program, the Justice Department began an investigation into the source of the leaked national security information.[121]

In an even more public confrontation, Treasury Secretary John W. Snow responded to the TFTP program disclosure by writing a letter to the editor to the *New York Times*, demonstrating the government's anger at its decision to publish the article.[122] Furthermore, at least one prominent member of the House of Representatives, then-Chairman of the House Homeland Security Committee Peter R. King, publicly advocated the government to seek criminal charges against "the New York Times—the reporters, the editors, and the publisher."[123] Days after the TFTP article, the House of Representatives formally voted to condemn the decision to disclose the program.[124]

While the decision by the *Times* to publish the existence and operation of the programs caused a firestorm of criticism of both the

---

120 Peter Baker & Charles Babington, *Bush Addresses Uproar over Spying* (Dec. 20, 2005), *available at* http://www.washingtonpost.com/wp-dyn/content/article/2005/12/19/AR2005121900211_pf.html (quoting President Bush, "[t]he fact that we're discussing this program is helping the enemy").

121 Toni Locy, *Justice Dept. Opens Domestic Spying Probe* (Dec. 30, 2005), *available at* http://www.breitbart.com/article.php?id=D8EQLIAGB&show_article=1. In August of 2007, the FBI searched the home of former Justice Department lawyer Thomas Tamm, taking his computer, two laptops, and some personal files; however, investigation continues and no charges have been brought against Mr. Tamm or any other person regarding the leak. Associated Press, *Report: FBI Searches Home of Attorney in Warrantless Wiretap Program Case* (August 5, 2007), http://www.foxnews.com/story/0,2933,292184,00.html (last visited Sept. 9, 2007).

122 John W. Snow, *Bank Data Report: Treasury Dept.'s View*, N.Y. TIMES, June 29, 2006, at A24. Secretary Snow asserted that the program was undermined by the disclosure, as terrorists were notified about America's method of tracking their financial activities. *Id*. Moreover, Secretary Snow assailed the *Times'* justification for publishing the article that the terrorists knew their money trails were being monitored by stating "[t]he fact that your editors believe themselves to be qualified to assess how terrorists are moving money betrays a breathtaking arrogance and a deep misunderstanding of this program and how it works." *Id*.

123 Devlin Barrett, *Lawmaker Wants Times Prosecuted* (June 26, 2006), *available at* http://www.washingtonpost.com/wp-dyn/content/article/2006/06/25/AR2006062500675.html.

124 Rick Klein, *House Votes to Condemn Media Over Terror Story* (June 30, 2006), *available at* http://www.boston.com/news/nation/articles/2006/06/30/house_votes_to_condemn_media_over_terror_story/?page=1. The nonbinding "Sense of the Congress" resolution states that the disclosure "may have placed the lives of Americans in danger" and that Congress "expects the cooperation of all news media organizations" in ensuring the secrecy of classified programs. *Id.* The resolution passed by a vote of 227-183, with seventeen Democrats joining almost all House Republicans in condemning the publication. *Id*.

government and the media, the *Times* may also have crossed a legal line.[125] As the aforementioned statutes and case law suggest, limits exist regarding the communication and publication of classified information.[126] Therefore, the next Part of this Note further explores whether the relevant law will allow such a prosecution of the *Times* for its publication of either the TFTP or NSA programs.[127]

III. ANALYSIS

The purpose of this Part is to demonstrate that while the Espionage Act may be ambiguous, the COMINT statute is straightforward, and strong policy rationales exist for enforcement of the latter's provisions.[128] First, Part III.A discusses the unambiguous nature of the COMINT statute, especially in comparison to other provisions of the Espionage Act.[129] Next, Part III.B analyzes the manner in which the COMINT statute protects sensitive national security information concerning intelligence, and also discusses the strong public policy for limiting the disclosure of confidential national security information.[130] Finally, Part III.C examines whether any of the provisions can or should apply to the disclosure of the classified TFTP or NSA programs by the *New York Times*.[131]

A. Espionage Act vs. COMINT Statute

In order to analyze the crucial differences between the Espionage Act and the COMINT statute, the actual wording of the provisions, legislative histories, and historical contexts must be examined.[132] By juxtaposing the words of the statutes, it is clear that as compared to the earlier enacted provisions, the COMINT statute is indeed "a model of precise draftsmanship."[133] The earlier Espionage Act included three major areas where ambiguity exists concerning the provisions' plain meaning.[134] First, there is uncertainty whether the publishing of information is the kind of communication that is necessary to satisfy an

---

125 *See infra* Part III.C.
126 *See supra* Part II.A-D.
127 *See infra* Part III.
128 *See infra* Parts III.A-C.
129 *See infra* Part III.A.
130 *See infra* Part III.B.
131 *See infra* Part III.C.
132 *See infra* Parts II.A-B.
133 Edgar and Schmidt, *supra* note 16, at 1065; *see also supra* notes 47-50 and accompanying text.
134 Edgar and Schmidt, *supra* note 16, at 938.

element of the statutes.[135] Additionally, the mens rea requirement that the information be willfully communicated with intent to injure the United States or to help another nation causes uncertainty, for it is a very subjective and malleable standard.[136] Finally, ambiguity exists perhaps to the greatest extent regarding the type of information that is protected by the statute, which includes the inherently ambiguous standard of "information 'relating to the national defense.'"[137]

In comparison, the COMINT statute contains straightforward language and definitions that allow very little room for misinterpretation.[138] For example, the provision explicitly includes the term "publishes" as a prohibition, and even sets it off by commas to possibly emphasize it.[139] Moreover, following the prohibitions of the COMINT statute, the drafters included precise definitions of the words "classified information," "communication intelligence," and "unauthorized person."[140] Because there is no statutory element that the United States be at war, it is clear that the section prohibits all such disclosures, regardless of the intricacies of modern day declarations of war.[141]

Additionally, the legislative histories and historical contexts of the statutes shed light on their purposes.[142] Congress had debated and unequivocally refused to criminalize the publishing of all types of defense information when it passed the precursors to the current Espionage Act in 1917.[143] However, the fact that Congress subsequently passed the COMINT statute after World War II and the *Chicago Tribune*'s

---

135 *Id.* (discussing the Espionage Act and its corresponding legislative history that causes confusion, since the plain language of sections 793(c)–(e) seems to criminalize almost any acquisition by journalists of information relating to the national defense; however, Congress "did not understand the provisions to have that effect, and they have never been so employed").

136 *Id.* at 1040 (determining that Congress did not fully appreciate the implications the Espionage Act would have upon activities that it had not deliberately wanted to criminalize).

137 *See supra* note 35 and accompanying text (describing how a plain reading of the statute could prohibit the publishing of any defense related information).

138 *See* Edgar & Schmidt, *supra* note 16, at 938.

139 *See supra* note 37 for the full text of the provision.

140 *Id.* The subsection also defines "code," "cipher," "cryptographic system," and "foreign government." *Id.* Such helpful definitions are lacking from the other main provisions of the Espionage Act. 18 U.S.C. §§ 793–794 (2000).

141 *See supra* note 50 and accompanying text; *see also* Edgar & Schmidt, *supra* note 16, at 1065.

142 *See supra* Parts II.A-B.

143 *See supra* notes 23-24 and accompanying text (describing the defeat of President Wilson's press censorship proposal).

disclosure of cryptographic information after the Battle of Midway gives overwhelming credence to the idea that Congress clearly meant to prohibit the publication of communications intelligence.[144] The protection of this nation's communications intelligence secrets were essential then, and the significance of their protection has only increased in the decades that have followed.[145]

B. It's Secret for a Reason

When the Espionage Act was first enacted, Congress had national security on its mind, because World War I had just ended.[146] Congress was again concerned with national security when it passed the COMINT statute soon after World War II.[147] Traditionally, the need to keep information secret has been the greatest in wartime, when there are troop, ship, and munitions movements, individual battle and long-term theater strategies are precious, and the appearance of unity among allies is essential.[148] Even at the outset of the Cold War, the Espionage Act was successfully applied, as it could be utilized proficiently against the classic spies who fit the common definitions of espionage and treason.[149]

However, history has shown in numerous, and seemingly constant, instances that declarations of war are not the only times when lives are lost and property is destroyed. For example, during the Cold War, the United States and the Soviet Union never officially declared war upon one another.[150] Yet, the nations indirectly fought various contests

---

144 *See supra* notes 39-43 and accompanying text; *see also* Schoenfeld, *supra* note 39, at 25 (explaining the way in which the *Chicago Tribune's* publication of codebreaking secrets following during World War II eventually led to the enactment of the COMINT statute).

145 *See infra* Part III.B.

146 *See supra* note 21 and accompanying text.

147 *See supra* notes 39-43 and accompanying text. The legislative histories of the statutes also indicate as much. *Id.*

148 E.E.B. & K.E.M., *Plugging the Leak: The Case for a Legislative Resolution of the Conflict Between the Demands of Secrecy and the Need for an Open Government*, 71 VA. L. REV. 801, 824 (1985). "[T]he maintenance of an effective national defense require[s] both confidentiality and secrecy. . . . In the area of basic national defense the frequent need for absolute secrecy is, of course, self-evident." N.Y. Times Co. v. United States, 403 U.S. 713, 728 (1971) (Stewart, J., concurring).

149 Martin, *supra* note 77, at 680. Perhaps the most unforgettable application of the Espionage Act occurred during the 1950s trial of Julius and Ethel Rosenberg following their furnishing of atomic bomb secrets to the Soviet Union. *Id.*

150 E.E.B. & K.E.M., *supra* note 148, at 824. Proxy wars occurred in Korea, Vietnam, Angola, and Central America. *Id.* Certainly, countless other surrogate battles were fought in other places, not only with lives, but with materials and financial assistance. *Id.*

around the world, where thousands of lives were lost and collateral destruction occurred.[151]

In these types of continuous struggles, interests and information beyond that pertaining to military operations must be kept from unintended nations and entities. Obviously important are defense installations and features of weapon systems.[152] Also, a nation's prewar contingency plans have not nearly the same value if enemies have such strategies, for the latter can neutralize any advantages of the plans by preparing countermeasures.[153] Additionally, certain nonmilitary technologies must also be protected during both peace and war, because advances in research and development correspond directly to military strength and battlefield success.[154]

Perhaps the most important secrecy interest is communications intelligence, because it deals with intelligence methods, sources, and operations.[155] This type of intelligence is crucial because its objective is to obtain information about foreign nations and entities, including military capacities, internal political atmosphere, and diplomatic options.[156] Accordingly, information gained via communications intelligence has the objectives of both guaranteeing efficient national defense and also maintaining an effective foreign policy.[157]

Protecting the means by which such information is gathered can be just as critical as the actual information that is collected. Keeping one's own nation's communications intelligence methods secret ensures that other nations or entities do not take substantive steps to stop the flow of its information.[158] Moreover, when an intelligence operation is ongoing, it is very susceptible to failure if it is disclosed, because of the obvious

---

151 *Id.*

152 *Id.* The most evident among these include nuclear, chemical, and biological weaponry.

153 *Id.*

154 *Id.* at 825.

155 *Id.*; *see also supra* note 39 (discussing a formal definition of COMINT). As compared to other types of strict intelligence, such as electronic intelligence and foreign instrumental signals intelligence, "COMINT is widely regarded as both the most prevalent and the most valuable intelligence." J. Terrence Stender, *Too Many Secrets: Challenges to the Control of Strong Crypto and the National Security Perspective*, 30 CASE W. RES. J. INT'L L. 287, n.220 (1998).

156 E.E.B. & K.E.M., *supra* note 148, at 825.

157 *Id.*

158 *Id.*

fact that the entity that is the object of the operation will almost certainly take countermeasures to block the flow of the targeted information.[159]

Following the terrorist attacks of September 11, 2001, it has become brutally clear just how magnified both the accumulation of intelligence about terrorist groups by means of communication intelligence has become, and also the importance of preventing those groups from becoming aware of the information-gathering techniques employed against them. As the enemies of the United States increasingly become groups that are not officially recognized nation-states, it is more difficult to identify the targets of intelligence, and thus more problematic to learn, among other things, of their military capabilities, possible future strikes, styles of recruitment, and comforting abettors.[160] Additionally, intelligence is clearly an essential way to enable the United States and its allies to find, pursue, and apprehend terrorists.[161] Furthermore, in contrast to the wars of previous generations, the war on terror has more at stake, for a failure in our intelligence of the enemy could lead to a new Pearl Harbor or September 11th calamity, but with the use of weapons of mass destruction in the place of dive bombers or hijacked airliners.[162]

It would be naïve to think that when terrorist organizations learn of the intelligence methods that the United States or its allies use, they

---

159 *Id.* The Supreme Court has tended to understand as much. *See, e.g.*, United States v. Nixon, 418 U.S. 683, 710 (1974) ("[t]he President, both as Commander-in-Chief and as the Nation's organ for foreign affairs, has available intelligence services whose reports are not and ought not to be published to the world") (quoting C. & S. Air Lines v. Waterman S.S. Corp., 333 U.S. 103, 111 (1948)); Snepp v. United States, 444 U.S. 507, 509 n.3 (1980) ("[t]he Government has a compelling interest in protecting both the secrecy of information important to our national security and the appearance of confidentiality so essential to the effective operation of our foreign intelligence service").

160 *Today's Realities in the War on Terror*, National Security Council Press Release, http://www.whitehouse.gov/nsc/nsct/2006/sectionII.html#challenges (last visited Feb. 13, 2008) (describing as one of the challenges of the War on Terror that "[t]errorist networks today are more dispersed and less centralized. They are more reliant on smaller cells inspired by a common ideology and less directed by a central command structure[.]" Additionally, terrorists' "[i]ncreasingly sophisticated use of the Internet and media has enabled our terrorist enemies to communicate, recruit, train, rally support, proselytize, and spread their propaganda without risking personal contact").

161 Schoenfeld, *supra* note 106, at 4; *see also* RICHARD A. POSNER, NOT A SUICIDE PACT 139 (2006) (explaining the high value of indirect intelligence in the fight against terrorism, hypothecizing examples of "an imam who, though not himself involved in terrorism, was preaching holy war . . .family members of a terrorist, who might have information about his whereabouts . . . sales invoices for materials that could be used to create weapons of mass destruction, or of books and articles that expressed admiration for suicide bombers").

162 Schoenfeld, *supra* note 106, at 4. Also, the fact that our society is so open leaves us "uniquely vulnerable." *Id.*

would not take countermeasures, just as a traditional nation would do.[163] In fact, terrorist organizations such as al Qaeda rely on information from media sources to a substantial extent.[164] An al Qaeda training manual, along with details about how to make bombs, take hostages, assassinate leaders, and withstand interrogation, also instructs how to obtain critical information about the societies that its members target:

> Using . . . public source[s] openly and without resorting to illegal means, it is possible to gather at least 80% of information about the enemy. The percentage varies depending on the government's policy on freedom of the press and publication. It is possible to gather information through newspapers, magazines, books, periodicals, official publications, and enemy broadcasts.[165]

The NSA program and the TFTP operation were two of the most important tools that the United States government used to gain crucial intelligence about al Qaeda and other terrorist organizations.[166] Utilized when international communications were discovered between a suspected terrorist and a person inside America, the information gathered was surely numerous and invaluable; Risen and Lichtblau's December 2005 article even pointed out that information collected by the program was used to apprehend terrorist Iyman Faris.[167] Similarly, the TFTP was especially helpful in curtailing the flow of funds to terrorist organizations.[168] Through the program, the government was able to

---

163 Rick Brundrett, *Gonzales Talks Tough Against Terrorists*, THE STATE, Jan. 12, 2007 (reporting that Attorney General Gonzales told his audience of U.S. Attorneys that "more needs to be done because terrorists 'change tactics in response to what we do'").

164 Laura K. Donohue, *Terrorist Speech and the Future of Free Expression*, 27 CARDOZO L. REV. 233, 234 (2005) (discussing the impact that the combination of the nature of technology and the freedom of expression in America and Great Britain is having on the ability of terrorists to obtain and disseminate critical information).

165 *Id.* at 234-35 (quoting an al Qaeda training manual salvaged from a safe house in Manchester, England). The manual goes on to assert that much other information can be gained from ordinary media, such as photographs of government personnel, information concerning economic vulnerabilities, access to secure buildings, location of water sources, observations of response times, and even prophylactic measures utilized by first responders. *Id.* at 235.

166 *See supra* notes 105-07 and accompanying text (describing the importance of the NSA program); *see also supra* notes 122-24 and accompanying text (asserting the necessity for the TFTP program).

167 *See supra* note 105 (explaining the terrorist plot of Faris).

168 Levey, *supra* note 115, at 1. "'[F]ollowing the money' is one of the most valuable sources of information that we have to identify and locate the networks of terrorists and their supporters." *Id.*

deter future donors by blocking the operations of a bogus charity or company, and also by arresting donors.[169] Additionally, the government followed the money trail to identify terrorist networks and their supporters and operatives.[170] Again, the details of successes stemming from the program remain top secret, but both Secretary Snow and Secretary Levey have each publicly hailed the program as, at least when functioning covertly, a highly effective tool.[171]

However, *New York Times* executive editor Bill Keller defended the publication of both articles.[172] Generally, he has asserted the obvious, yet powerful, point that the freedom of the press is central to the First Amendment and that the media holds a unique role as watchdog over government activities.[173] More specifically, Keller has maintained that the terrorists, before the disclosure, could not have been so naïve as to believe that their international communications were not being traced.[174] He utilized this same argument regarding the decision to disclose the

---

169 *Id.*

170 *Id.*

171 Snow, *supra* note 122, at A24 (calling the program "a robust and classified effort to map terrorist networks . . . [I] sought to impress upon him [Mr. Keller] the great value the program had in defeating terrorism"). *See also* Levey, *supra* note 115, at 3-4:

> I have received the written output from this program as part of my daily intelligence briefing. For two years, I have been reviewing that output every morning. I cannot remember a day when that briefing did not include at least one terrorism lead from this program. Despite attempts at secrecy, terrorist facilitators have continued to use the international banking system to send money to one another, even after September 11th. This disclosure compromised one of our most valuable programs and will only make our efforts to track terrorist financing—and to prevent terrorist attacks – harder. Tracking terrorist money trails is difficult enough without having our sources and methods reported on the front page of newspapers.

Id. at 3-4.

172 *See, e.g.*, Bill Keller, *Letter from Bill Keller on The Times's Banking Records Report*, N.Y. TIMES, June 25, 2006; Transcript, The Situation Room, *Interview With Bill Keller; Bomb Threat Forces Closure of Major American Port*, CNN.COM, June 26, 2006, http://transcripts.cnn.com/TRANSCRIPTS/0606/26/sitroom.03.html (last visited Feb 14, 2008).

173 *See generally* Keller, *supra* note 172.

174 Schoenfeld, *supra* note 39, at 31. However, there are examples where terrorists have continued to be seemingly naive. As previously mentioned, the NSA program has produced results since September 11th, including the discovery ofinternational communications between terror suspects and Iyman Faris. *See supra* note 105. It also uncovered another al Qaeda plan to bomb British pubs and train stations in 2004 partly from information obtained via the NSA program. *See* Risen & Lichtblau, *supra* note 99, at A1. These examples were even included in the story the Times' published, thus it seems erroneous for the executive editor to later claim that the terrorists must be too intelligent to communicate via international communications. Schoenfeld, *supra* note 39, at 31.

TFTP program.[175] However, regardless of the strength of the policy arguments offered by each viewpoint, pertinent statutes and case law must be examined to determine whether the *New York Times* can be prosecuted for their disclosure of the classified programs.[176]

C. The Possibilities of Prosecution

Relatively recent case law over the past several decades has suggested that a prosecution under a statute such as this would not be unfathomable.[177] At least four Justices asserted in the Pentagon Papers case that prosecutions against reporters and publishers could be permitted.[178] However, when such was attempted against reporters Ellsberg and Russo, it was not judged on its merits.[179] Furthermore, in *United States v. Morison*,[180] the court found that even the ambiguous Espionage Act could be applied to a media-related situation, as opposed to the classic case of turning over classified information to an agent of a foreign government.[181] Further indicating that the courts are willing to protect national security secrets, AIPAC officials are currently being prosecuted for obtaining classified information and conspiring to pass it along to other diplomats and the media.[182] Again, the conduct of persons who are involved in their professional activity as lobbyists and who are not government employees who pass protected information to others, is, in certain respects, very similar to the conduct of the *New York Times*.[183]

Among the provisions of the Espionage Act that may allow a prosecution, the logical place to begin is section 793(e), which prohibits one who has "unauthorized possession of . . . information relating to the national defense" which could be "used to the injury of the United

---

175 *See generally* Keller, *supra* note 172.

176 *See infra* Part III.C.

177 *See supra* Parts II.C, II.D.

178 *See supra* notes 61-68 and accompanying text; *see also* N.Y. Times Co. v. United States, 403 U.S. 713 (1971).

179 *See supra* notes 69-73 and accompanying text (describing the events surrounding the attempted prosecution of Ellsberg and Russo); *see also* United States v. Russo, No. 9373-(WMB)-CD (filed Dec. 29, 1971), *dismissed* (C.D. Cal. May 11, 1973).

180 844 F.2d 1057 (4th Cir. 1988).

181 *See supra* notes 78-84 and accompanying text (discussing the *Morison* case and its implications on the application of the Espionage Act).

182 United States v. Rosen, 445 F. Supp. 2d 602 (E.D. Va. 2006); *see also supra* notes 85-97 and accompanying text (explaining the AIPAC case and its repercussions on national security situations).

183 *See supra* notes 95-97 and accompanying text (examining the similarities between Rosen and Weissman and the disclosures of the *New York Times*).

States" from "willfully communicat[ing] . . . the same to any person not entitled to receive it . . . ."[184] Although many of the terms used in the statute are inherently vague, if the statute is given a broad understanding, the disclosures by the *New York Times* seem to fit under the plain meaning of the statute.[185] Because both programs were illegally leaked to Risen and Lichtblau, their possession was unauthorized, and they willfully communicated details of the classified information when the stories were published.[186] Finally, terrorists who read the articles are not persons entitled to receive the information, thus its disclosure could have caused injury to the United States, and the publication of the stories on the front page of a major national newspaper was a communication of the information.

Bluntly stated, however, section 793(e) has never been applied as the plain meaning suggests that it could be.[187] The legislative history of the Espionage Act as a whole gives the most compelling reasons for this.[188] In 1917, Congress explicitly refused to enact a provision that would have prohibited publications of national defense information, and after a heated debate, instead ratified the ambiguous language that largely survived until today.[189] When amended in 1950, Congress then passed the narrow COMINT statute, again inferentially refusing to enact a broad press censorship provision.[190] As a result, it should be concluded that the Espionage Act could not be utilized to successfully prosecute Risen, Lichtblau, Keller, or the publisher of the *New York Times*.

The analysis, of course, cannot stop there, for the applicability of the COMINT statute is another possibility for prosecution. After examining the plain meaning of the words in the statute that applies to, "[w]hoever

---

184 18 U.S.C. § 793(e) (2000); *see supra* note 29 for entire text of the statute.

185 *See supra* Part III.A (discussing the ambiguous nature of the provision).

186 However, the criminal element "willfully" has been called "chameleon-like," where its meaning seems to change depending on the context of its application. *See* Sharon L. Davies, *The Jurisprudence of Willfulness: An Evolving Theory of Excusable Ignorance*, 48 DUKE L.J. 341, 380 n.155 (1998).

187 Edgar & Schmidt, *supra* note 16, at 1032. "On their face, however, the purposes of subsections 793(d) and (e) are mysterious because the statutes are so sweeping as to be absurd." *Id.*

188 *See supra* note 34 and accompanying text (discussing the legislative history of the Espionage Act).

189 *Id.*

190 *See supra* notes 44-46 and accompanying text. "Doubts that the legislative history justifies the conclusion that Congress saw a general distinction between communication and publication are reinforced because the distinction is not theoretically sound in the context of the espionage statutes and cannot be applied in any sensible fashion." Edgar & Schmidt, *supra* note 16, at 1035.

knowingly and willfully . . . publishes . . . any classified information . . . concerning the communication intelligence activities of the United States. . .," prosecution is a very viable option for the disclosure of the NSA program.[191] The disclosure was knowing and willful and was accomplished by means of publishing on the front page of a national newspaper.[192] Moreover, the *New York Times* knew the program was a highly classified governmental secret that had been leaked to it.[193] Finally, the element that requires that the subject of the disclosure concern communications intelligence also is met, as the NSA program seems to be exactly what Congress had in mind when it included the term "communications intelligence" in the definition section of the statute.[194]

Furthermore, the legislative history of the COMINT statute is particularly helpful in this situation.[195] The *Chicago Tribune* incident during World War II is eerily similar to the disclosure of the NSA program, as each of them instructed the United States' deadly enemies of the methods by which America was gathering information about them, and they both occurred during armed conflicts.[196] When the COMINT statute was enacted in 1950, it was in direct response to the *Tribune* incident, and it logically follows that Congress thought that the narrow category of press censorship mandated by the provision was necessary to maintain national security, into which the NSA program plainly fits.[197]

However, it does not seem that the disclosure of the TFTP program could be applied in a similar fashion. Just as the Espionage Act is vague as applied to the NSA disclosure, it is also ambiguous in terms of the TFTP operation.[198] Under the Espionage Act, the subject matter of the communication is not the crucial element, but rather the means by which

---

191 18 U.S.C. § 798(a) (2000); *see supra* note 37 for the full text of the statute.

192 *See generally supra* Part II.E.

193 Risen & Lichtblau, *supra* note 99, at A1. "Nearly a dozen current and former officials, who were granted anonymity because of the classified nature of the program . . . ." *Id.*

194 18 U.S.C. § 798(b) (2000). "The term 'communication intelligence' means all procedures and methods used in the interception of communications and the obtaining of information from such communications by other than the intended recipients." *Id.*; *see also supra* note 37 (for the full text of the statute).

195 *See supra* notes 38-46 and accompanying text (describing the legislative history of the COMINT statute).

196 *See supra* notes 39-42 and accompanying text (explaining the historical setting in which the COMINT statute was passed).

197 *Id.*

198 *See supra* Part III.A (discussing the vagueness of the Espionage Act).

the communication occurred, and Congress did not intend for publishing to be criminalized.[199]

Additionally, the COMINT statute cannot be applied to the publishing of the TFTP operation either. While the statute does prohibit publishing, nowhere in the COMINT statute does the provision mandate the prosecution for the disclosure of the subject matter of financial intelligence.[200] In 1950, Congress made a conscious choice by limiting the censorship of the press to the narrow field of communications intelligence and code systems.[201] It can thus be inferred that Congress did not believe the rights of the press should be curtailed to limit the publishing of other classified information, including economic tracking and monitoring systems.[202]

The Espionage Act was amended in 1950 after the *Chicago Tribune* incident shook the nation and Congress' collective conscience, as Congress had determined that the media utilized excessive discretion in its decision to publish the secret of the breaking of the Japanese code.[203] Over half a century later, it is possible that history similarly taught Congress that the time has come to update the Federal Criminal Code to prohibit journalists from publishing other categories of classified intelligence information.

IV. CONTRIBUTION—A NECESSARY UPDATE

Current federal statutes that allow criminal charges to be brought against those who publish certain types of confidential national security intelligence information are insufficient in today's post-September 11th world.[204] Specifically, while the COMINT statute can be applied to publishers of communications intelligence such as the disclosure of the NSA warrantless wiretap program, neither it nor the Espionage Act includes provisions that allow for prosecution of persons or entities that publish other confidential intelligence information.[205]

---

199 *See supra* note 135 (describing the uncertainty as to whether the prohibitive scope of the Espionage Act reaches publication).

200 18 U.S.C. § 798 (2000); *see supra* note 37 (for the full text of the statute).

201 *Id.*

202 *See supra* note 144 (explaining the narrow focus of the COMINT statute).

203 *See supra* notes 39-44 (discussing the direct relationship between the *Chicago Tribune* article and the COMINT statute).

204 *See supra* Part III.

205 *See supra* Part III.C.

Therefore, this Note proposes an additional statute to the Federal Criminal Code that prohibits the publishing of classified government programs that deal with the tracking and following of suspected terrorists' financial activities.[206] The statute, which could be located in the Code after the related provisions at 18 U.S.C. § 800, is based largely from the COMINT statute, as its wording is unambiguous and narrow.[207] With the twin goals of plugging a current breach in national security laws, while still protecting the freedom of the press, the following statute is proposed:

A. Proposed 18 U.S.C. § 800[208]

> (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 *concerning the financial intelligence activities* of the United States or any foreign government shall be fined under this title or imprisoned not more than ten years, or both.
>
> (b) As used in subsection (a) of this section –
>
> The term "classified information" means information which, at the time of a violation of this section, is, for reasons of national security, specifically designated by a United States Government Agency for limited or restricted dissemination or distribution;
>
> 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

---

206 *See infra* note 208.

207 *See supra* notes 138-41 and accompanying text (discussing the focused language and scope of the COMINT statute).

208 With the exception of the italicized language, the language of the proposed statute has been reproduced from the statutory language of the COMINT statute and its corresponding definitions.

> within a foreign country, whether or not such government is recognized by the United States;
>
> *The term "financial intelligence activities" means all procedures and methods used in the monitoring of information related to financial data obtained from international financial institutions;*
>
> The term "unauthorized person" means any person who, or agency which, is not authorized to receive information of the categories set forth in subsection (a) of this section, by the President, or by the head of a department or agency of the United States Government which is expressly designated by the President to engage in financial intelligence activities for the United States.
>
> (c) Nothing in this section shall prohibit the furnishing, upon lawful demand, of information to any regularly constituted committee of the Senate or House of Representatives of the United States, or joint committee thereof.
>
> (d) Any person convicted of a violation of this section shall forfeit, to the United States irrespective of any provision of State law –
>
> (1) any property constituting, or derived from, any proceeds the person obtained, directly or indirectly, as the result of such violation; and
>
> (2) 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.

B. Commentary

The goal of proposed section 800 is to allow the prosecution of persons, including journalists and publishers, who disclose confidential programs or methods utilized by the government to monitor the transfers of funds that often occur in correspondence with terrorist activities. As a shadowy enemy without an official nation, it is quite difficult to employ traditional methods to successfully discover the actions and future plans of terrorist organizations and individuals. Often, the best way to gain intelligence about terrorists is to observe the

residual effects of their actions, which include their manners of communications and means of funding their operations. The COMINT statute prohibits the disclosure of classified programs that gain communications intelligence, and proposed section 800 will ban the disclosure, including the publishing, of manners of tracing financial activities.

In addition, proposed section 800 will not unconstitutionally abridge the freedom of the press. As at least four justices mentioned in the Pentagon Papers case, the Espionage Act, even with all of its troublesome statutory language, could in theory be applied to criminally prosecute journalists who disseminate certain government secrets.[209] Thus, because the language of proposed section 800 is unambiguous, includes definitions for potentially unclear terms, and is much more focused than the Espionage Act, the provision will pass a constitutional challenge on vagueness or overbreadth grounds and the judiciary also should have no hesitation in applying it. Furthermore, both *Morison* and the recent AIPAC case indicate that courts will faithfully apply enacted statutes, especially when national security interests are at stake.[210]

Moreover, similar to the COMINT statute, section 800 is an extremely targeted provision that seeks not to silence the press, but instead to protect vital anti-terrorist interests.[211] Just as when Congress passed the COMINT statute to target disclosures similar to the *Chicago Tribune*'s publishing of cryptographic information in World War II, Congress would clearly intend section 800 to apply only to disclosures similar to the TFTP revelation, as the legislative history and Congressional debate would undoubtedly indicate.[212] As a result, there would be no fear that section 800 would suppress the media from making any comments on national defense information, as the broad and defeated provision offered by the Wilson administration to Congress in 1917 would have done.[213] Such would be neither the intent nor the result of the proposed legislation.

The tracking and combating of terrorist finances is a critical tool in the war on terror, and proposed section 800 would arm the government with a weapon that could allow it to fight the war without unnecessary

---

209 *See supra* Part II.C.

210 *See supra* Part II.D.

211 *See supra* Part III.A.

212 *See supra* Part II.B.

213 *See supra* notes 23-24 and accompanying text (examining the defeat of the Wilson administration's press censorship proposal).

interference from journalists. After all, "[t]racking terrorist money trails is difficult enough without having our sources and methods reported on the front page of newspapers."[214]

In total, proposed section 800 serves two important purposes. First, it fills a void in the Criminal Code by prohibiting the disclosure, particularly the publishing, of classified information regarding a crucial weapon in the war on terror, the tracking of terrorist finances. As the war on terror is an unconventional war, it follows that unconventional methods must be utilized to give America its best opportunity for victory, and monitoring the money trail of terrorists is a critical weapon. Certainly, our enemies should not be able to learn of our classified methods of fighting terror by simply subscribing to the *New York Times*. Second, proposed section 800's plain language and clear legislative history would unambiguously indicate that the freedom of the press is not unnecessarily abridged, as only a narrow, yet important, subject matter is prohibited from disclosure. In sum, section 800 would impede American journalists from distributing this nation's anti-terror secrets, while at the same time not unnecessarily abridging the freedom of the press.

V. CONCLUSION

As wars and conflicts evolve, so must the laws of the United States progress to ensure the survival and safety of its citizens. Congress has done this in the past, as its enacted statutes regarding the disclosure of classified information have developed to guard against certain transgressions. The statute that is proposed in this Note is a continuation of that development. Instead of attempting a strained and misguided application of the Espionage Act, proposed section 800 would prohibit journalists from giving away narrow yet crucial secrets that have been illegally leaked to them through backchannels. By passing such legislation, our newspapers at home, disenchanted leakers in the government, and our enemies abroad would realize that the United States government will not tolerate the disclosure of its secrets, whether traded in the dead of the night by spies or publicized in its newspapers. In a world where everyday is September 12, Congress should not wait for the occurrence of the nightmare scenario presented in Part I before it gets serious about fighting terrorism. This Note's proposed statute would be one small, yet necessary, step in the right direction towards

---

214 Levey, *supra* note 115, at 3-4.

ensuring that the situation recounted in Part I remains only a hypothetical.

Mark R. Alson[215]

[215] J.D. Candidate, Valparaiso University School of Law, 2008; B.A., Classical Civilization, DePauw University, 2005. I would like to thank my parents, Dan and Gayle, and my brother, Adam, for their lifelong support. Additionally, I would like thank Professor Nuechterlein for her help during the Notewriting process, and I extend my appreciation to the members of the Valparaiso Law Review for their dedication.