

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND**

UNITED STATES OF AMERICA

*

v.

*

Criminal No. 1:10-cr-0181-RDB

THOMAS ANDREWS DRAKE

*

**DEFENDANT’S MOTION TO DISMISS COUNTS 1-5 OF THE
INDICTMENT BECAUSE 18 U.S.C. § 793(e) IS UNCONSTITUTIONALLY
VAGUE AS APPLIED AND OVERLY BROAD UNDER THE FIRST AMENDMENT**

The defendant, Thomas Drake, through his attorneys, respectfully moves this Court to dismiss Counts One through Five of the Indictment. These five counts allege that Mr. Drake violated 18 U.S.C. § 793(e) by maintaining unauthorized possession of certain documents and willfully retaining them. This statute is unenforceable as written. No court has approved its plain language as providing fair notice of what conduct the statute proscribes. *See United States v. Morison*, 844 F.2d 1057 (4th Cir. 1988); *United States v. Rosen*, 445 F. Supp. 2d 602 (E.D. Va. 2006). Prosecuting Thomas Drake under this statute violates the fair notice requirements of the Due Process clause because multiple terms contained in Section 793(e) are so vague that they fail to provide him with notice of what conduct is criminal and what conduct is not. In addition, the statute is unconstitutionally overbroad under the First Amendment.

- The statute seeks to impose a criminal penalty on those who willfully retain documents relating to the national defense. But the phrase “relating to the national defense” covers such a massive quantity of information that the statute fails to draw a clear line between criminal and non-criminal conduct. *See United States v. Lanier*, 520 U.S. 259, 265 (1997).
- Section 793(e) fails to identify with the requisite specificity what constitutes a culpable state of mind. *See Rosen*, 445 F. Supp. 2d at 626-27.
- Section 793(e) states that conduct is criminal if a person retains information that the person has reason to believe could be used to the injury of the United States. This

phrase is also unconstitutionally vague.

- The statute seeks to impose criminal penalties on those who retain or disclose information in a way that threatens “the ability of the press to scrutinize and report on government activity.” *Morison*, 844 F.2d at 1081 (Wilkinson, J., concurring). This means that the statute is highly likely to restrict protected speech, and that the restriction is socially significant. Because a substantial number of the statute’s applications restrict protected speech, 18 U.S.C. § 793(e) is overly broad under the First Amendment. *See United States v. Stevens*, 130 S. Ct. 1577, 1587 (2010).
- The wide scope of 18 U.S.C. § 793(e) appears to criminalize the communicative activities of whistleblowers, like Mr. Drake, and reporters who work with them. These individuals by definition engage in speech on topics of public concern, such as exposing fraud, waste, abuse, inefficiency, or corruption within the government. The First Amendment provides special protection to those whose speech acts touch on such topics.

WHEREFORE, for these reasons, which are explained in detail in the accompanying Memorandum, and for other reasons that may be developed at the hearing on this Motion, this Court should dismiss Counts 1 through 5 of the Indictment.

Respectfully submitted,

/s/

JAMES WYDA, #25298
Federal Public Defender
DEBORAH L. BOARDMAN, #28655
Assistant Federal Public Defender
MEGHAN SKELTON
Staff Attorney
Office of the Federal Public Defender
100 South Charles Street
Tower II, Ninth Floor
Baltimore, Maryland 21201
Phone: 410-962-3962
Fax: 410-962-0872
Email: Jim_Wyda@fd.org
Deborah_Boardman@fd.org
Meghan_Skelton@fd.org

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND**

UNITED STATES OF AMERICA

*

v.

*

Criminal No. 1:10-cr-0181-RDB

THOMAS ANDREWS DRAKE

*

**DEFENDANT’S MEMORANDUM IN SUPPORT OF MOTION
TO DISMISS COUNTS 1-5 OF THE INDICTMENT BECAUSE 18 U.S.C. § 793(e)
IS UNCONSTITUTIONALLY VAGUE AS APPLIED AND OVERLY BROAD UNDER
THE FIRST AMENDMENT**

The Defendant, Thomas Drake, through his attorneys, respectfully moves this Court to dismiss Counts One through Five of the Indictment. These five counts allege that Mr. Drake violated 18 U.S.C. § 793(e) by maintaining unauthorized possession of certain documents and willfully retaining them. This statute is unenforceable as written. No court has approved its plain language as providing fair notice of what conduct the statute proscribes. *See United States v. Morison*, 844 F.2d 1057 (4th Cir. 1988); *United States v. Rosen*, 445 F. Supp. 2d 602 (E.D. Va. 2006). This statute is described as “so sweeping as to be absurd” and bearing constitutional flaws that “go well beyond tolerable limits.”¹ The statute is unconstitutionally vague and overbroad.

INTRODUCTION

Section 793(e), one of the espionage statutes and a relic of World War I, last modified during the Cold War, is “undoubtedly the most confusing and complex of all the federal espionage statutes.”

¹ Harold Edgar and Benno C. Schmidt, Jr., *The Espionage Statutes and Publication of Defense Information*, 73 Colum. L. Rev. 929, 1031-32 (1973) (hereinafter *The Espionage Statutes*). This article is the most comprehensive resource on the espionage statutes in existence. It details the legislative history of the precursor statutes of 1911 and 1917, and examines each section of the 1950 amendments in depth. Only a handful of reported decisions post-date this article. Accordingly, despite publication date of 1973, it remains an essential tool in analyzing this statute. A copy is attached as Exhibit A.

The Espionage Statutes, 73 Colum. L. Rev. at 998. “Unfortunately, they are also the statutes that pose the greatest threat” to the freedom of the press. *Id.* If wading through the confusion identified by courts and commentators alike when considering this statute is possible, avoiding the sweeping breadth of the statute is impossible. Despite the significant First Amendment problems that the statute raises, the legislation “is at its scattergun worst precisely where greatest caution should have been exercised.” *Id.*

Section 793(e) is unenforceable as written.² Indeed, no court has found that its plain language satisfies the notice requirements of due process. *See Morison*, 844 F.2d at 1086 (Phillips, J., concurring) (concluding that the statute is both constitutionally overbroad and vague, but reluctantly agreeing despite having “grave doubts” that the limiting instructions brought the statute within a constitutional orbit). Multiple of its terms are so vague as to violate due process, thereby failing to give Mr. Drake fair notice of what conduct the statute proscribes. The literal meaning of the statute is sweeping and “almost certainly unconstitutionally vague and overbroad,” but “the statutory language does not point toward any one confined reading as a means of saving them.” *The Espionage Statutes*, 73 Colum. L. Rev. at 1000. Although several courts have tried to impose some definition and limits on the breadth of its sweep in order to rescue the statute from the widely-acknowledged vagueness, these attempts cannot save the statute. These attempts at limitation far

² *Id.* *See also United States v. Morison*, 844 F.2d 1057 (4th Cir. 1988) (finding the statute unconstitutionally vague as written and requiring significant judicial interpretation to allow prosecution under the statute). *See also* Melville B. Nimmer, *National Security Secrets v. Free Speech: The Issues Left Undecided in the Ellsberg Case*, 26 Stan. L. Rev. 311, 325 (1974) (hereinafter Nimmer, *Free Speech*) (statute fatally overbroad and cannot be fixed via judicial construction); *see also The Espionage Act and the Legal and Constitutional Issues Raised By Wikileaks*, Hearing Before the House Committee on the Judiciary, December 16, 2010, Prepared Statement of Stephen I. Vladek (a copy of this statement is attached as Exhibit B).

exceed imposing a “judicial gloss” on the statute, which can sometimes bring a vague statute within an acceptable sphere of definition, but have instead reached the level of judicial re-drafting of the statute. This has essentially created a federal common law crime. This the Constitution does not allow. The statute is unconstitutionally vague and continuing with this prosecution would violate Mr. Drake’s rights under the Due Process Clause of the Fifth Amendment.

Not only is Section 793(e) so vague as to violate due process as applied to Mr. Drake, but it is also overly broad under the First Amendment. The statute criminalizes core political speech – here, an attempt at an open discussion and exposure of fraud, waste and abuse by a government agency. The statute also improperly proscribes the freedom of the press by criminalizing the retention of documents and information necessary for the press to inform the public about the government’s conduct and to engage in debate about governmental policies. While the government certainly has an interest in protecting national security, Section 793(e) is not narrowly tailored to achieving that legitimate governmental interest.

The Fourth Circuit has recognized the significance of the First Amendment interest at stake and jeopardized by this statute: “Criminal restraints on the disclosure of information threaten the ability of the press to scrutinize and report on government activity. There exists the tendency, even in a constitutional democracy, for government to withhold reports of disquieting developments and to manage news in a fashion most favorable to itself. Public debate, however, is diminished without access to unfiltered facts.” *Morison*, 844 F.2d at 1081 (Wilkinson, J., concurring). This statute, however, restricts the free flow of information to the press, and impedes the American public’s ability to engage in debate based on knowledge rather than ignorance. *See id.* Its reach is too broad,

and the significance of the First Amendment interest at stake is too great.³ The statute therefore fails on First Amendment grounds as well. This Court should therefore dismiss Counts One through Five.

BACKGROUND⁴

Thomas Drake has devoted most of his career to serving his country, first, in the Tactical Air Command of the United States Air Force and, most recently, as a Senior Executive with the National Security Agency (NSA). In late August of 2001, Mr. Drake joined NSA as the Chief of the Change Leadership and Communications Office in the Signals Intelligence Directorate. Mr. Drake's duties at NSA focused primarily on changing process and improving efficiency.

In January of 2003, Mr. Drake was contacted by investigators from the Department of Defense Inspector General's Office and asked to serve as a witness for an extensive, year-long investigation into a complaint of fraud, waste, and abuse at NSA. Specifically, the complaint alleged that NSA's actions in the development of the program TRAILBLAZER resulted in waste, fraud, and abuse. The complaint also alleged that NSA had disregarded the program THINTHREAD, which was a more viable and cost-effective solution to urgent national security needs. Mr. Drake agreed with the allegations in the complaint.

Mr. Drake cooperated closely, properly, and extensively in support of the investigation into waste, fraud, and abuse. There are hundreds of e-mail exchanges between Mr. Drake and the investigators, many of them accompanied by substantial attachments from Mr. Drake. He met with

³ The significant First Amendment interest at stake renders the statute all the more suspect on due process grounds. Because the statute criminalizes speech, the due process demands of precision and notice to the accused are substantially heightened.

⁴ This Court should not read this summary of the facts and description of allegations included in the Indictment as a concession that they are true.

the investigators, in person, on numerous occasions. Frequently, Mr. Drake hand-delivered documents to the investigators.

In 2004, after more than a year of fact-finding, the Inspector General issued its audit findings in a report entitled “Requirements for the TRAILBLAZER and THINTHREAD Systems.” Mr. Drake were right. An unclassified copy of this report states that “the National Security Agency is inefficiently using resources to develop a digital network exploitation system that is not capable of fully exploiting the digital network intelligence available to analysts from the Global Information Network.” The Inspector General concluded that “the NSA transformation effort may be developing a less capable long-term digital network exploitation solution that will take longer and cost significantly more to develop.” The NSA, however, continued investing in the flawed system.

Several newspaper articles⁵ discussed these failings and the wasted government funds. The Indictment alleges that Mr. Drake was one of the sources of information for these newspaper articles.⁶ *See* Indictment ¶ 13. The Indictment alleges that Mr. Drake willfully retained five different documents. These documents are a handful of pages in a virtual sea of paper in Mr. Drake’s home. These five documents, about fifteen pages, were recovered amidst thousands of documents, and many thousands of pages, either in miscellaneous stacks of paper from the floor of Mr. Drake’s basement or from computer files. Paragraphs 9-14 of the Indictment explicitly allege that Mr. Drake’s motive to retain these documents was to share them with Reporter A. Each of the documents related in some degree to the programs in question and the issues at stake in the Inspector

⁵ *See, e.g.,* Siobhan Gorman, *NSA Rejected System That Sifted Phone Data Legally, Dropping of Privacy Safeguards After 9/11, Turf Battles Blamed*, Baltimore Sun at 1A (May 18, 2006) (2006 WLNR 8539601).

⁶ The newspaper articles themselves identify multiple sources for each article.

General audit.

Notably, the government does not allege that Mr. Drake is a spy who intended to harm his country. He is not. This case is not about the retention of documents or disclosure of information relating to, for example, troop movements, weapons systems, satellite images, or identities of covert operatives. Instead, it is about a citizen who was deeply troubled by his government's waste of money and NSA's refusal to engage in the most effective intelligence gathering at its disposal. The documents at issue in this case concern NSA's waste, fraud, and abuse. Most importantly, Mr. Drake's activities relating to these documents were intended to reveal the waste, fraud, and abuse that cost the taxpayers money, weakened our civil liberties, and hindered our nation's ability to identify potential threats against our security.

ARGUMENT

I. SECTION 793(e) IS UNCONSTITUTIONALLY VAGUE.

Counts One through Five charge Mr. Drake with violations of 18 U.S.C. § 793(e). That statute imposes a criminal penalty on “[w]hoever having unauthorized possession of, access to, or control over any document . . . 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 retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it[.]” The statute defines none of its terms.

Commentators and courts alike conclude that this statute, as written, is seriously constitutionally flawed. Although some courts have attempted to construe the statute so that it will not violate the Due Process Clause, those attempts have failed. In particular, the clauses “relating

to the national defense;” “reason to believe that the information could be used to the injury of the United States;” and “willfully retains” are all unconstitutionally vague. No judicial gloss can save this vague statute.

Because the vagueness doctrine is an “as applied” doctrine, the same statute may be unconstitutionally vague in one case, but may not run afoul of the Due Process Clause in another. Section 793(e) and similar subsections of the espionage laws provide examples. This statute, first enacted in 1917 and then modified in 1950, has typically been used as a tool to prosecute those who we consider “spies”; most of the reported cases in the past 50 years involved conduct that did not occur at the margins of constitutionality. Instead, most of the reported decisions involve clear-cut scenarios, like stealing documents relating to weapons systems and selling those documents to agents of the U.S.S.R. *See, e.g., United States v. Walker*, 796 F.2d 43 (4th Cir. 1986); *United States v. Kampiles*, 609 F.2d 1233 (7th Cir. 1979); *United States v. Lee*, 589 F.2d 980 (9th Cir. 1979). But this case is anything but clear-cut. And no pre-existing judicial gloss on 18 U.S.C. § 793(e) has drawn a clear line between the conduct Mr. Drake allegedly engaged in and conduct that would be lawful.

The Fourth Circuit has previously held that Section 793(e) is not unconstitutionally vague as applied to a different individual who disclosed satellite images to the press. *See Morison*, 844 F.2d at 1071-72. The court reached that conclusion only because the trial judge had given certain jury instructions limiting the broad *mens rea* and narrowing the meaning of “national defense.” *Id.* Although *Morison* is certainly instructive, in that it concludes that the statute cannot be applied as written and identifies at least two elements that must be limited before enforcement of the statute can proceed, the case does not control the instant case. Two of the judges deciding *Morison* explicitly

noted the necessity of “judicious case-by-case use of appropriate limiting instructions[.]” *Id.* at 1086 (Phillips, J., concurring); *see also id.* at 1084-85 (Wilkinson, concurring) (leaving open distinct possibility that statute could not be constitutionally applied to those “who truly expose governmental waste and misconduct”; emphasizing that case does not involve application of espionage statute to facts relating to the press and classified materials). One judge nevertheless expressed “grave doubts about the sufficiency of the limiting instructions[.]” *Id.* at 1086 (Phillips, J., concurring). And in the 25 years since that case was decided, other courts have weighed in on the questionable elements of 793(e), narrowing them beyond what the Fourth Circuit mentioned in *Morison*. *See, e.g., Rosen*, 445 F. Supp. 2d at 626.

Moreover, the conduct at issue in *Morison* is sufficiently different from the conduct at issue here that limiting instructions that may have provided *Morison* with fair notice of the statute’s reach will not provide Mr. Drake with the same fair notice. Although *Morison* involved a leak to the press, it did not involve a whistleblower like Mr. Drake. The defendant in *Morison* had stolen satellite photos of a Russian aircraft carrier and sold the photos to the press for personal monetary gain. *Morison*, 844 F.2d at 1061. Here, on the other hand, Mr. Drake had been involved with an inspector general’s investigation of fraud, waste, and abuse by the NSA – an investigation that concluded the NSA was in fact wasting money and failing to efficiently process raw intelligence data. The documents at issue all relate to his whistleblowing activities. Mr. Drake stood nothing to gain from retaining or disclosing this information; he could only lose. He believed, however, that the country as a whole stood to gain from pressure brought to bear on the NSA to begin operating less wastefully and more efficiently. Thus, *Morison* is certainly not the final word on the subject of the vagueness of 18 U.S.C. § 793(e).

A. Due Process Requires a Criminal Statute to Draw a Clear Line Between What is Criminal and What is Lawful Conduct.

The Due Process Clause of the Fifth Amendment requires that any law that imposes criminal liability must give potential defendants fair warning of what conduct is proscribed. Criminal liability cannot be imposed without “fair warning . . . in language that the common world will understand of what the law intends to do if a certain line is passed. To make the warning fair, so far as possible the line should be clear.” *United States v. Lanier*, 520 U.S. 259, 265 (1997) (quoting *McBoyle v. United States*, 283 U.S. 25, 27 (1931)). Due process “bars enforcement” of a statute that uses “terms so vague that men of common intelligence must necessarily guess at its meaning and differ as to its application.” *Id.* at 266 (quoting *Connally v. General Constr. Co.*, 269 U.S. 385, 391 (1926)).

When examining a statute with vague terms, courts may impose a “judicial gloss” to supply the “clarity at the requisite level . . . on an otherwise uncertain statute[.]” *Id.* This “gloss,” however, is limited. First, due process prevents a court from applying a novel construction of a criminal statute in any given case; the statute, standing alone or as previously construed, must make it reasonably clear at the time that the defendant engages in the conduct targeted by the prosecution that the conduct was criminal. *Id.*; *see also id.* at 265 n.5 (describing the principle that conduct may not be treated as criminal unless it has been so defined by a competent authority before the conduct has occurred).

Second, the “gloss” must be just that – minor clarifications and limitations. “Federal crimes are defined by Congress, not the courts[.]” *Id.* at 267 n.6 (citation omitted). A judicial construction of a statute cannot effectively re-draft the legislation. The “judicial gloss” may only go so far as

necessary to give effect to congressional intent. *See id.* A court “may impose a limiting construction on a statute only if it is readily susceptible to such a construction.” *Reno v. American Civil Liberties Union*, 521 U.S. 844, 884 (1997) (quotation omitted). This gloss cannot add omitted terms or redefine existing ones. A court cannot “rewrite a . . . law to conform it to constitutional requirements.” *Id.* at 884-85 (quotation omitted). Courts that have interpreted Section 793(e) in the past have had to rewrite the statute, adding omitted terms, and changing others. As discussed below, even with the existing constructions of the statute, Section 793(e) fails to give fair notice under the Due Process Clause.

B. The *Mens Rea* Element of Section 793(e) is Unconstitutionally Vague.

Section 793(e) seeks to proscribe the willful retention of certain documents. But “willful,” as applied to Mr. Drake, is unconstitutionally vague. “‘Willful’ is one of the law’s chameleons, taking on different meaning in different contexts.” *The Espionage Statutes*, 73 Colum. L. Rev. at 1038 (footnote omitted). Although the term “willful” certainly requires a specific intent to violate the law, a more precise definition of willfulness is not provided in this statute. Courts and commentators alike agree that some additional limitation on the culpable intent addressed by Section 793(e) is necessary, lest it fail to survive due process scrutiny. But there has been no agreement as to what is required.⁷

Although the Supreme Court has never addressed the scienter requirement of Section 793(e), it has discussed the intent element in the precursor statute that included some of the identical terms.

⁷ *See Rosen*, 445 F. Supp. 2d at 625-27; Hearing Before the Senate Committee on the Judiciary, Subcommittee on Terrorism and Homeland Security, *The Espionage Act: A Look Back and a Look Forward*, written testimony of Stephen I. Vladeck (p. 9 (May 12, 2010)) (attached as Exhibit C) (describing the *mens rea* requirement in the statute as “lax”).

In *Gorin v. United States*, 312 U.S. 19 (1941), the Court read the term willfulness in connection with the phrase “intent or reason to believe that the information to be obtained is to be used to the injury of the United States, or to the advantage of a foreign nation.” *Id.* at 27-28, 32 n.17. The Court held “[t]his requires those prosecuted to have acted in bad faith.” *Id.* at 28. Thus, the Supreme Court held that the government must prove an evil motive or bad purpose on the part of the defendant in order for the prosecution to satisfy the scienter requirement of the Espionage Statutes. *Id.* See also *Hartzel v. United States*, 322 U.S. 680, 686 (1944) (holding that “willfulness” as used in the Espionage Statutes require proof of “a specific intent or evil purpose” – deliberately narrowing the scienter requirement because of the restrictions on the freedom of expression occasioned by the statutes); see also *United States v. Squillacote*, 221 F.3d 542, 577 (4th Cir. 2000) (describing the scienter element of the Espionage Statutes as requiring “those prosecuted to have acted in bad faith”) (quotation omitted); *Morison*, 844 F.2d at 1071 (approving a jury instruction on the intent element of Section 793(e) – without much analysis regarding willfulness – requiring a “bad purpose”) (quotation omitted).

The most recent decision to interpret the scienter required by Section 793(e) is *United States v. Rosen*, where the court held that Section 793(e) imposes “an additional and significant scienter requirement” over and above the standard definition of “willfulness.” 445 F. Supp. 2d at 625. Like in *Gorin*, the court analyzed the term “willfully” in conjunction with the phrase “reason to believe” that disclosing or retaining the information would injure the United States. The Court concluded that a standard specific intent jury instruction would be insufficient to save Section 793(e) from unconstitutional vagueness. The court reasoned that specific intent alone – acting with the knowledge that the conduct violated the law and the knowledge that disclosing the information could

threaten national security – would nevertheless encompass conduct that the defendant may have undertaken with “some salutary motive.”⁸ *Id.* at 626. Accordingly, the court held that Section 793(e) includes an additional scienter requirement: the government must prove that the defendant disclosed the information “with a bad faith purpose to either harm the United States or to aid a foreign government.” *Id.* See also *Nimmer*, 26 *Stan. L. Rev.* at 325 (“[F]ailure to require an intent to injure the United States or aid a foreign nation makes the provision relating to disposition of documents fatally overbroad.”) (footnote omitted). Thus, Section 793(e) included not simply a specific intent to do something the law prohibited, but also to engage in that conduct with “bad faith” and an evil motive. *Rosen*, 445 F. Supp. 2d. at 626-27. See also *United States v. Truong Dinh Hung*, 629 F.2d 908, 919 (4th Cir. 1980) (rejecting the possibility that the offense could be committed negligently or by mistake and holding that the intent element of a related statute requires proof that the defendant acted “willfully and with an intent or reason to believe that the information would be used to injure the United States or to aid a foreign power” and requiring the proof that the conduct was “prompted” by some “underhanded motive.”).

Although it may be tempting to agree with the court in *Rosen* that Section 793(e) can be saved by reading a scienter into the statute that includes the evil motive discussed in *Gorin* and requires the government to establish beyond a reasonable doubt that the defendant acted with more than simple willfulness, also acting with the intent to injure the United States or aid a foreign nation, this Court should not do so. Including this scienter element is more than adding a “judicial gloss” to the statute; it requires the court to rewrite the statute and add omitted terms. “Given the clear

⁸ Here, Thomas Drake, a whistleblower, certainly acted with a salutary motive. Exposing waste and inefficiency in the government is at the core of what the First Amendment seeks to protect.

statutory language, the statement of legislative intent, and the prior construction of this language by the Supreme Court, it seems clear that a trial court could not narrowly construe [either Section 793(d) or (e)] in order to save it from constitutional invalidity without in effect rewriting it.” Nimmer, *Free Speech*, 26 Stan. L. Rev. at 325-26.

The legislative history suggests that Congress did not intend a special meaning for “willfully” in this statute.⁹ Although Sections 793(a) and (b) require a *mens rea* that the defendant act with the “purpose or knowledge that the primary use to which information will be put is the injury of the United States or the advantage of a foreign nation,” Section 793(e) does not include the same explicit limitation. *The Espionage Statutes*, 73 Colum. L. Rev. at 1046.¹⁰ Although courts and commentators have concluded that a similar interpretation for “willfulness” is necessary to save Section 793(e) from vagueness, the text and legislative history does not indicate that Congress intended this. *Id.*

Because of the constitutional flaws in this statute, “courts struggling with [this] defect have reached disparate conclusions as to the requisite *mens rea* that individuals must have to violate the Act.” Vladeck, *supra* note 2 at 2. “Undeniable but poorly articulated constitutional concerns have compelled courts to read into the statute requirements that aren’t supported by its language.” *Id.* The fact that courts have reached different conclusions, as discussed in commentary on this statute, means that the statute is not “readily susceptible” to a limiting construction. *Reno*, 521 U.S. at 884

⁹ For an in depth discussion of the legislative history regarding the term “willfully,” see *The Espionage Statutes*, 73 Colum. L. Rev. at 1038-46.

¹⁰ See also Vladeck Prepared Statement, *supra* note 2 at 1-2 (“[T]he plain text of the Act fails to require a specific intent either to harm the national security of the United States or to benefit a foreign power.”).

(quotation omitted). This Court should not rewrite the law in order to conform it to the Constitution. *Id.* at 884-85. Instead, this Court should dismiss Counts One through Five as unconstitutionally vague.

C. The Phrase “Relating to the National Defense” is Unconstitutionally Vague.

Section 793(e) prohibits the willful retention of documents or information “relating to the national defense.” This statutory phrase is also unconstitutionally vague because it does not give fair notice of what documents or information an individual may not disclose or unlawfully retain. *See Squillacote*, 221 F.3d at 576 (“The statutes at issue unfortunately provide no guidance on the question of what kind of information may be considered related to or connected with the national defense.”).

The Supreme Court examined this phrase in the precursor statute to Section 793(e). The Court held that the words “national defense” carry a meaning of “a generic concept of broad connotations, referring to the military and naval establishments and the related activities of national preparedness.” *Gorin*, 312 U.S. at 28 (quotation omitted); *see also Morison*, 844 U.S. at 1071 (defining “national defense” broadly). The Court approved a jury instruction providing a broad definition of “national defense,” and including the admonition that “the connection [between the information and the national defense] must not be a strained one nor an arbitrary one. The relationship must be reasonable and direct.” *Gorin*, 312 U.S. at 31 (quotation omitted). Regarding Section 793(e), the *Rosen* court noted that the phrase has “consistently been construed broadly to include information dealing with military matters and more generally with matters relating to United States foreign policy and intelligence capabilities.” 445 F. Supp. 2d at 620.

But this limiting construction of the phrase has been deemed insufficient to narrow the statute to constitutional requirements. *Id.* Information that “refer[s] to the military and naval establishments” includes innocuous information of alarming breadth. *United States v. Heine*, 151 F.2d 813, 815 (2d Cir. 1945) (quotation omitted) (explaining that the *Gorin* definition includes railway maps, lists of engineering schools, and the average yield of arable land). “There are innumerable documents referring to the military or naval establishments, or related activities of national preparedness, which threaten no conceivable security or other government interest that would justify punishing one who ‘communicates’ such documents.” Nimmer, *Free Speech*, 26 Stan. L. Rev. at 326. Because the statute has such weighty First Amendment implications, prohibiting the disclosure or retention of information so broadly defined, even if done with the culpable scienter discussed above, could not withstand constitutional scrutiny. Therefore, courts have taken a series of steps to narrow the meaning of the phrase.

One of the first of these steps is to limit the information to that which is not public – limiting the reach of the statutes to information that is “closely held” by the government. If the information already exists in the public domain, it cannot qualify as “relating to the national defense” under 18 U.S.C. § 793(e). Information that is “lawfully available to the general public does not relate to the national defense.” *United States v. Dedeyan*, 584 F.2d 36, 40 (4th Cir. 1978). The Fourth Circuit has approved a jury instruction that defines the term as limiting the disclosure of information and documents that are “closely held in that they have not been made public and are not available to the general public.” *Morison*, 844 F.2d at 1071-72 (bracket and ellipses omitted) (footnote omitted).

Nevertheless, these judicially imposed constraints on the broad statutory phrase fail to narrow the statute to within the limits that due process requires. The statutory phrase remains

unconstitutionally vague because these limits do not cabin the type of information sufficiently to give a possible defendant fair notice of what information or documents may not be possessed, disclosed, or retained. Even requiring that the document or information be classified fails to provide notice of what the statute covers. The executive branch does not exercise the classification system with any clarity. *The Espionage Statutes*, 73 Colum. L. Rev. at 1052. And the limitation fails to address situations “where individuals disclose classified information that should never have been classified in the first place, including information about unlawful government programs and activities.” Vladeck, *supra* note 2 at 4. Stamps on a document identifying it as classified “are at most circuitous references” to regulations other than the Espionage Act and do not give meaning to the phrases within that Act. *The Espionage Statutes*, 73 Colum. L. Rev. at 1057.

As discussed above, courts have thus reached different conclusions regarding the meaning of the phrase “relating to the national defense.” Continually dissatisfied with the limitations placed on the phrase by earlier decisions, succeeding opinions add more and more refinements to the definition. The phrase therefore is not amenable to a limiting construction without judicial rewriting of the phrase. *See Reno*, 521 U.S. at 884-85. The phrase remains unconstitutionally vague. Any further limiting of the definition now would be to impose a novel construction on a statute – a construction not in place when the alleged conduct occurred. That would also render the statute unconstitutionally vague. This Court should therefore dismiss Counts One through Five because they fail to give fair notice of what type of information the possession, disclosure, or retention of which is criminal.

D. The Phrase “Injury to the United States or to the Advantage of any Foreign Nation” is Unconstitutionally Vague.

A third way in which 18 U.S.C. § 793(e) fails to provide fair notice of what conduct constitutes a crime, and what conduct does not, is in the phrase “injury to the United States or to the advantage of any foreign nation.” Under the plain terms of the statute, conduct is criminal if the person possesses, communicates, or retains information and the person has reason to believe that the information could be used to “the injury of the United States.” This phrase is also constitutionally flawed.

Initially, the fact that the phrase is written in the disjunctive, covering either information that could injure the United States or aid a foreign nation, creates a sweep of such breadth as to violate the Constitution. It criminalizes conduct that does not injure the United States, yet may provide some advantage to a foreign nation. *See Nimmer, Free Speech*, 26 Stan. L. Rev. at 330. “But if a communication does not work an injury to the United States, it would seem to follow logically that no government interest can be asserted to overcome the first amendment’s guarantee of freedom of speech.” *Id.* (footnote omitted).

No existing judicial gloss saves this phrase. Courts use the phrase when they infer a scienter requirement – reasoning that evil motive, bad purpose, and acting with the intent to injure the United States is the *mens rea* necessary to save the statute from the constitutional graveyard. *See, e.g., Rosen*, 445 F. Supp. 2d at 625-26; *Truong Dinh Hung*, 629 F.2d at 918-20. But the actual statute uses the phrase to describe the type of information, not the state of mind. The phrase modifies “relating to the national defense.” The statute lists the types of documents it covers, so long as they relate to the national defense, then continues, “or information [in addition to documents] 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.” 18 U.S.C. § 793(e) (emphasis added). Moreover, because the phrase has been judicially transferred to describing the *mens rea* rather than the type of information covered by the statute, any attempt to define the scope of the statute necessarily become increasingly circular. Each term and element can only be defined using the other terms and elements. Therefore, no judicial interpretation of the statute serves to clarify any of the vague terms.

The judicial constructions that delete the statutory phrase modifying the scope of information covered by the Act, *see Nimmer, Free Speech*, 26 Stan. L. Rev. At 330, and use it as a modifier to the culpable intent, obscure an element of the offense and constitute one of the most significant constitutional flaws in the statute. Under the plain terms of the statute, the government must prove that the defendant has reason to believe that disclosing or retaining the documents or information could injure the United States or aid a foreign nation, but the statute fails to provide any guidance on what that injury or aid must be. Moreover, no judicial construction of the statute identifies the type or magnitude of injury at issue.

As noted below, a significant government interest must be implicated in order to justify abridging an individual’s First Amendment rights and criminalize speech, as Section 793(e) does. Yet the Espionage Act fails to identify what that interest is or how significant the injury must be. The bare bones language in Section 793(e) is too general to survive First Amendment scrutiny. “Since such a standard would never be acceptable in other speech contexts, there is no reason that it should be more acceptable where the antispeech interest is national security.” *Nimmer, Free Speech*, 26 Stan. L. Rev. at 331. The First Amendment requires that “there must be ‘narrow,

objective, and definite standards to guide” criminal enforcement. *Id.* (quoting *Shuttlesworth v. Birmingham*, 394 U.S. 147, 151 (1969)). There are no guideposts here, only that the defendant has reason to believe that disclosure of the information could injure the United States or aid a foreign nation. These statutory requirements, however, is far too abstract a standard to satisfy this requirement. There is nothing “narrow, objective, or definite” about the phrase or the limits on the type of information that would bring disclosure within the realm of criminal conduct.

Justice Brennan’s opinion in the Pentagon Papers case discusses the type of injury to the United States that could trigger a governmental interest sufficient to overcome an individual’s First Amendment rights. *See New York Times v. United States*, 403 U.S. 713, 725-27 (1971) (Brennan, J., concurring). The First Amendment tolerates no “surmise or conjecture” when considering harm to the United States. *Id.* at 725. “[M]ere conclusions” by the executive branch that the government would be harmed or that disclosure of the information *would* or *could* injure the United States is insufficient. *Id.* at 727. Instead, “only governmental allegation and proof that publication must inevitably, directly, and immediately cause the occurrence of an event kindred to imperiling the safety of a transport already at sea can support even the issuance of an interim restraining order.” *Id.* at 726-27. An abstract, undefined injury, that “could” occur – as described by 18 U.S.C. § 793(e) – fails to even approximate this standard.

The phrase “injury to the United States or to the advantage of any foreign nation” fails to restrict the type of information covered by Section 793(e) with sufficient clarity to provide a defendant with fair notice of what constitutes criminal conduct. The phrase is too abstract. Moreover, it contemplates punishing conduct even when no identifiable government interest is harmed. No judicial construction limits the phrase; the only constructions of the phrase employ it

as a means of creating an additional scienter requirement, rendering any further use of the phrase circular. Using the phrase in this way simply highlights the significant constitutional problems with the statute. The phrase leaves only conjecture and surmise about what the government must prove in order to secure a conviction. That conjecture and surmise is insufficient to give fair notice under the Due Process Clause.

E. The Combination of Constitutional Flaws Renders 18 U.S.C. § 793(e) Unconstitutionally Vague.

It seems that no phrase within 18 U.S.C. § 793(e) can be read without defining it in reference to another phrase in the same statute. No statute thus limited can provide fair notice of the line between criminal and non-criminal conduct.

Yet, when courts attempt to parse the statutory phrases individually, the general conclusion is that the statute is void for vagueness. The term “willfully” cannot stand on its own, but must be limited with additions imposed by courts and borrowing from parts of the statute that address elements other than *mens rea*. Likewise, the term “relating to the national defense” cannot stand on its own. Courts have imposed increasingly narrow constructions of the phrase to avoid absurd results. These frequent attempts at avoiding absurd results, however, simply demonstrate that the statutory requirements, including prior constructions, fail to give fair notice of what conduct constitutes a crime. And “injury” has evaded judicial construction, except insofar as it now apparently modifies scienter. The type and degree of injury or aid remain an abstract notion that could cover topics as wide as embarrassing the party in power for gaffes during televised interviews to identifying members of the CIA’s clandestine service operating in war zones. The terms fail to give narrow, objective, and definite delineations of the type of injury, harm to the government, or

aid to a foreign nation that triggers enforcement of the Espionage Act.

The statute is not amenable to judicial construction. Courts continue to differ about the meaning of the different phrases and continue to find that the phrases are not specific enough. People of common intelligence have to guess at the meaning of this statute and are likely to disagree about the definitions of the elements discussed above. This means that the statute is unconstitutionally vague. *See Lanier*, 520 U.S. at 266. The judicial interpretations that have occurred so far are not a mere “gloss,” but instead require a broad revision and redrafting of the statute to render it constitutional. The statute is unconstitutionally vague.

The rule of lenity requires that any ambiguity in a criminal statute must be resolved in the defendant’s behalf. *See Abbott v. United States*, ___ U.S. ___, 131 S. Ct. 18, 31 n.9 (2010). The ambiguities in Section 793(e) are legion. Resolving them in favor of Mr. Drake requires this Court to dismiss Counts One through Five.

II. SECTION 793(e) IS UNCONSTITUTIONALLY OVERBROAD UNDER THE FIRST AMENDMENT

Not only is 18 U.S.C. § 793(e) unconstitutionally vague as applied to Thomas Drake, but it is also overbroad under the First Amendment. A statute is overbroad if a substantial number of its applications are unconstitutional. *United States v. Stevens*, ___ U.S. ___, 130 S. Ct. 1577, 1587 (2010). When a statute is highly likely to restrict protected speech, and that restriction is socially significant, the statute is particularly suspect and almost certainly violates the First Amendment. *See Morison*, 844 F.2d at 1075 n.30.

The restriction on protected speech caused by 18 U.S.C. § 793(e) is both highly probable and socially significant. This Indictment makes the First Amendment implications explicit when in

Paragraphs 9-14 it alleges that Mr. Drake's motive was to "leak" these documents to Reporter A. This prosecution highlights at least two different ways that the statute chills protected speech. First, it violates Mr. Drake's First Amendment rights, as well as the rights of other whistleblower government employees who wish to engage in public debate and expose waste and inefficiencies in the government. Second, it violates the freedom of the press to investigate and publish articles relating to governmental policies.¹¹ This prosecution in particular – and the statute in general – criminalize core political speech, which is anathema to the First Amendment.¹²

A. Section 793(e) Regulates Protected Speech.

Congress has no power to regulate speech and restrict expression because of the message, content, ideas, or subject matter of the speech. *Stevens*, 130 S. Ct. at 1584. Section 793(e), which proscribes the disclosure or retention of documents or information "relating to the national defense" criminalizes speech based on its content. *See Turner Broadcasting Syst., Inc. v. FCC*, 512 U.S.

¹¹ A criminal defendant may litigate both the damage done to his own First Amendment rights by a prosecution, as well as the chilling of free speech by the press. *See Maryland v. Joseph H. Munson Co., Inc.*, 467 U.S. 947, 956 (1984) (permitting litigants to challenge a statute as violating another's free expression under a statute if that statute's "very existence may cause others not before the court to refrain from constitutionally protected speech or expression.") (quotation omitted).

¹² Counsel is aware that the Fourth Circuit concluded that 18 U.S.C. § 793(e) is not overbroad in *United States v. Morison*, 844 F.2d 1057 (4th Cir. 1988). Counsel, however, respectfully suggests that *Morison* does not control the result in this case. First, *Morison* is factually distinguishable in that the speech at issue was prompted by motives of private financial gain, rather than engaging in core political speech and opening discourse on a topic of national concern. *Id.* at 1085 (Wilkinson, concurring). The decision does not discuss whistleblowers – an area rife with particular First Amendment concerns. Second, since that decision, the Supreme Court has spoken on facial overbreadth challenges to criminal statutes in *United States v. Stevens*, 130 S. Ct. 1577 (2010). The Court has also addressed the First Amendment rights of government employees in *Garcetti v. Ceballos*, 547 U.S. 410 (2006). The Fourth Circuit has not yet addressed Section 793(e) in light of the most recent Supreme Court precedent. Mr. Drake's challenge to the overbreadth of the statute is therefore not foreclosed.

622, 642-43 (1994) (describing legislation that identifies disfavored speech in terms of its contents as a content-based regulation, even if it does not favor one viewpoint over another). If the disclosure or contents of the documents or information unlawfully retained does not address “the national defense” (however that phrase may be interpreted), then the speech is not regulated. But once the topic of the document or information is determined to relate to the national defense, then speech concerning those documents is regulated. Restrictions on speech based on its content, such as the one at issue here, are presumptively invalid; the government bears the burden of rebutting that presumption. *Stevens*, 130 S. Ct. at 1584.

Some restrictions on the content of speech do not violate the First Amendment. But these restrictions are limited to situations where the speech lacks expressive value. *See id.* at 1585. Speech about government programs, policies, spending, and public affairs, on the other hand, is core political speech that merits the greatest First Amendment protection. *Connick v. Myers*, 461 U.S. 138, 145 (1983) (describing speech about public affairs as “more than self expression” but rather “the essence of self-government” and having “the highest rung on the hierarchy of First Amendment values”) (citations omitted). The right to “examine and criticize government policies is at the core of the constitutionally guaranteed freedom of speech and press.” Anthony Lewis, *National Security: Muting the “Vital Criticism,”* 34 U.C.L.A. L. Rev. 1687, 1690 (1987) (hereinafter Lewis, *Muting Criticism*).

B. Speech Touching on Topics Relating to National Security Carries First Amendment Protection.

The fact that speech relates to documents or information that are classified or addresses issues of national security does not eliminate First Amendment protection. To be sure, the

government has an interest in protecting national security, but that interest does not trump the First Amendment. “Secrecy in government is fundamentally anti-democratic, perpetuating bureaucratic errors. Open debate and discussion of public issues are vital to our national health.” *New York Times*, 403 U.S. at 724 (Douglas, J., concurring). “[T]he only effective restraint upon executive policy and power in the areas of national defense and international affairs may lie in an enlightened citizenry – in an informed and critical public opinion which alone can here protect the values of democratic government.” *Id.* at 728 (Stewart, J., concurring). Judge Wilkinson sounded this same theme in his concurrence in *Morison*:

The First Amendment interest in informed popular debate does not simply vanish at the invocation of the words “national security.” National security is public security, not government security from informed criticism. No decisions are more serious than those touching on peace and war; none are more certain to affect every member of society. Elections turn on the conduct of foreign affairs and strategies of national defense, and the dangers of secretive government have been well documented.

Morison, 844 F. 2d at 1081 (Wilkinson, J., concurring). Thus, the government cannot insulate itself from public criticism – either by its employees or by the press – simply by reciting the mantra that the information or documents are classified and relate to national security.

The government’s interest in “national security” does not negate an individual’s First Amendment right to free expression or the freedom of the press. “[N]ational Security should not be used as a weapon to prevent employees from speaking out about matters traditionally protected by the First Amendment and whistleblower statutes, such as fraud, mismanagement, abuse of authority, and threats to the public safety.” Jamie Sasser, *Silenced Citizens: The Post-Garcetti Landscape for Public Sector Employees Working in National Security*, 41 U. Rich. L. Rev. 759, 782 (2007)

(hereinafter Sasser, *Silenced Citizens*).

Courts should grant the executive no special deference in First Amendment challenges to statutes simply because the restricted and chilled speech and publication relates to issues of national security.¹³ If courts were to defer to the executive whenever the First Amendment and national security intersected, the judicial “policy would deprive citizens of the opportunity to understand, evaluate, and vote on official conduct.” *The Espionage Statutes*, 73 Colum. L. Rev. at 934. Although national security may be an issue of particular concern to the executive, the courts are charged with protecting the liberties enumerated in the Bill of Rights. The doctrine of separation of powers requires each of the three branches to “guard its own prerogatives, resisting aggrandizement by the other branches.” Lewis, *Muting Criticism*, 34 U.C.L.A. L. Rev. at 1692. “The Separation of Powers and the First Amendment in its central meaning – are together being severely tested these days. For as the Executive Branch has grown to dominance, so has it tried to control information: tried to limit public examination of its activities.” *Id.* The executive’s jealous guarding of its secrets hardly makes allowances for the free expression of ideas, criticism of national policies, and prompting of public debate spurred by the press.

“[I]f the determination of government secrecy is made by executive fiat based on *no* principled ground – then such determination cannot pass constitutional muster.” Nimmer, *Free Speech*, 26 Stan. L. Rev. at 329. That determination – whether our constitutional rights are protected

¹³ Judge Wilkinson in his concurrence in *Morison* believed that he was ill-equipped to decide issues of national security and posited that he should defer to the executive. *Morison*, 844 F.2d at 1082 (Wilkinson, J., concurring). This Court should not be swayed by his reluctance to decide the important First Amendment issue. *See Stevens*, 130 S. Ct. at 1591 (explaining that Court would never defer to executive branch of government based only on its assurances that it would enforce laws in such a way as to not violate anyone’s First Amendment rights).

– is made by the judiciary, not the executive. “[T]he First Amendment protects against the Government; it does not leave us at the mercy of *nobless oblige*. We would not uphold an unconstitutional statute merely because the Government promised to use it responsibly.” *Stevens*, 130 S. Ct. at 1591 (citation omitted).

Here, Mr. Drake engaged in public criticism. He was not motivated by private financial gain – he never sold any information. Instead, he was prompting public debate about waste and inefficiency at NSA. The Indictment describes an individual’s and a newspaper’s criticism of wasteful government policies, mismanagement of government funds, and failures to analyze intelligence data in the best possible way (thereby potentially sacrificing national security).¹⁴ The Indictment thus describes speech of the highest First Amendment caliber. The government may not insulate itself from Mr. Drake’s criticism by claiming that the information related to national security. *New York Times*, 403 U.S. at 724 (Douglas, J., concurring). And this Court should not shy away from identifying the First Amendment weakness of Section 793(e) simply because the Executive Branch declares that the topics of Mr. Drake’s and the press’s expression touched on issues of national security.

¹⁴ See Siobhan Gorman, *NSA Rejected System that Sifted Phone Data Legally*, Baltimore Sun at 1A, 2006 WLNR 8539601, (May 18, 2006) (explaining that the NSA focused its efforts in a “far less capable and rigorous program” than what was available, and that doing so “undermined the agency’s ability to zero in on potential threats”).

C. Whistleblowers Like Thomas Drake, and Reporters Who Work With Them, Both of Whom by Definition Engage in Speech of Public Concern, Deserve Special First Amendment Protections.

The wide umbrella of the Espionage Act prohibits traditional whistleblowing activity. Anyone who willfully discloses or retains information relating to the national defense (however this may be interpreted) has committed a crime. The statute provides no exemption for an employee who may discover fraud, waste, or abuse in an area that relates to the national defense. An employee who then retains or discloses documents relating to that fraud, waste, or abuse has violated the statute. Similarly, the reporter who researches fraud, waste, and abuse in government programs that involve the national defense violates this statute when she obtains, discusses, retains, discloses or publishes the national defense information. The reach of this statute is too broad. Although the government may have an interest in protecting national security, it has no legitimate interest in preventing the dissemination of information about its own incompetence or corruption. The Espionage Act is therefore overly broad. It is not narrowly tailored to achieve a legitimate government interest, and it infringes on the First Amendment.

Section 793(e) includes no protection for whistleblowers like Mr. Drake or the reporters who publish stories relating to government waste or misconduct.¹⁵ But the government should not be able to insulate itself from criticism in such a manner. The First Amendment interests of the individual and the press are too high in this type of context to permit the chilling effect of imposing criminal penalties for engagement in the protected speech. Moreover, the public has a substantial interest in hearing the informed views of government employees engaging in civic discussion on topics of national concern. *See Pickering v. Board of Educ. of Township High School Dist. 205*, 391 U.S. 563,

¹⁵ *See* Vladeck, *supra* note 2 at 3.

572-73 (1968).

The Supreme Court has noted that, although a public employer may limit an employee's speech as it relates to the employee's job, it may not limit the speech as it relates to whistleblowing. "Exposing governmental inefficiency and misconduct is a matter of considerable significance . . . reinforced by the powerful network of legislative enactments – such as whistle-blower protection laws and labor codes – available to those who seek to expose wrongdoing. . . . These imperatives, as well as obligations arising from any other applicable constitutional provisions and mandates of the criminal and civil laws, protect employees[.]" *Garcetti*, 547 U.S. at 425-26.

When addressing the protections that whistleblower statutes might provide to government employees, the Supreme Court did not consider the breadth of the Espionage Act on employees who work in national security fields. The Court assumed that these protections were in place to prevent chilling of public employee speech when the employees sought to expose wrongdoing, *see id.*, but in fact the whistleblower laws do not protect employees of the NSA. *See Sasser, Silenced Citizens*, 41 U. Rich. L. Rev. at 780-81; *see generally*, Louis Fisher, Congressional Research Service, National Security Whistleblowers (2005) (available at <http://fas.org/sgp/crs/natsec/RL33215.pdf>) (explaining the substantial interest that the legislative branch has in receiving information from executive branch whistleblowers on topics of critical national concern, such as defense cost overruns, unsafe nuclear power plants, and contractor illegalities, but the difficulties in obtaining it because of the paucity of protections for these whistleblowers). Those who provide this vital information – often only knowledgeable because of their positions in government – deserve First Amendment protection for adding to the public debate on issues of national policy and government activity.

The need to provide whistleblowers with First Amendment protection is heightened by the

fact that the legislative history of the Espionage Act demonstrates that Section 793(e) was not intended to apply to the press. The 1917 Act explicitly rejected proposals that would punish publication of national defense information. *The Espionage Statutes*, 73 Colum. L. Rev. at 1032. When the statute was amended in 1950, “the notion that somehow newspapers were not covered . . . was never challenged.” *Id.* at 1033. Therefore, Section 793(e) “cannot be held applicable to publication of defense information that is motivated by the routine desires to initiate public debate or sell newspapers, unless this congressional purpose, confirmed by repeated subsequent refusals to enact broad prohibitions on disclosures, is ignored.” *Id.* (footnote omitted). *See also* Laura Barandes, *A Helping Hand: Addressing New Implications of the Espionage Act on Freedom of the Press*, 29 Cardozo L. Rev. 371 (2007) (explaining the unconstitutionality of applying Section 793(e) to the press). Other statutes that do reach publication, do so explicitly. *Compare* 18 U.S.C. § 794(b) (“Whoever, in time of war, with intent that the same shall be communicated to the enemy, collects, records, *publishes* or communicates . . .”) (emphasis added); 18 U.S.C. § 797 (titled “Publication and sale of photographs of defense installations”); 18 U.S.C. § 798(a) (explicitly delineating publishing as one of the ways to violate the statute).

If publishing the information in the press was never meant to be covered by the statute, then the activities of the press incidental to publication – such as retaining documents or information or gathering information from whistleblowers – must also fall outside the scope of the statute. “If it is conceded that Congress meant to exclude publication from criminal prohibitions pertaining to communications, it is inconceivable that they would contemplate making criminal retentions incident to that act[.]” *The Espionage Statutes*, 73 Colum. L. Rev. at 1037. And once the press’s retention of documents or information is deemed outside the scope of the statute, a government employee

source for the press is likewise outside the scope. *Id.* (explaining that Congress could have enacted a statutory scheme whereby the press was exempted, but a government employee was not, but “the espionage statutes do not, however, enact such a system”). Instead, government employee disclosures of secrets to the press are exempted just as the publication is.

D. Not all Disclosures of Secret Information Bearing on National Security By Government Whistleblowers Would Receive the Same First Amendment Protection.

Whistleblowers stand in a different position relative to the First Amendment than other government employees who may unlawfully disclose or retain information relating to the national defense. Many of the prosecutions under the espionage statutes of government employees addressed situations where individuals undoubtedly sought to injure the United States and aid a foreign government. *See Squillacote*, 221 F.3d 542; *United States v. Abu-Jihaad*, 600 F. Supp. 2d 362 (D. Conn. 2009). Government whistleblowers, on the other hand, are individuals with the best possible knowledge on topics of foreign and domestic policy, government practices, and fraud, waste, and abuse within government. Motivated to remedy these problems, they provide information to individuals outside their own agencies or to the press as a means of opening public debate. This type of speech is the pinnacle of what the First Amendment protects.

But courts and the government need not face a Hobson’s Choice of allowing all disclosures of information that relate to the national defense because of the First Amendment protections due to whistleblowers. Some disclosures of national defense information or unlawful retention of particular documents can and will remain proscribed. A standard that protects the governmental interest in safeguarding national security while still protecting individuals’ freedom of expression and the freedom of the press could exist. A standard could balance the speech and anti-speech

interests. *See Pickering*, 391 U.S. at 572-73. “Where communicative activities occur with the intent to achieve a public disclosure to the American people (as distinguished from a private disclosure to an agent of a foreign nation) then it seems proper to conclude that such activities may be the subject of criminal punishment only if a ‘serious injury’ to the state can be proven to be both likely and imminent as a result of such public disclosure, as the Supreme Court has required in other free speech contexts.” Nimmer, *Free Speech*, 26 Stan. L. Rev. at 331-32 (footnotes omitted). This standard approximates the one suggested by Justice Brennan in the Pentagon Papers case, that “publication must inevitably, directly, and immediately cause the occurrence of an event kindred to imperiling the safety of a transport already at sea[.]” *New York Times*, 403 U.S. at 726-27 (Brennan, J., concurring).

Therefore, as discussed above, the statute proscribes too much protected speech. The likelihood that it will chill protected expression is too great. The statute is overbroad on its face. This Court should therefore dismiss Counts One through Five.

III. IN THE ALTERNATIVE, THE COURT MUST PROVIDE LIMITING INSTRUCTIONS THAT NARROW THE BREADTH AND DEFINE THE VAGUE TERMS.

If this Court disagrees with Mr. Drake and concludes that Section 793(e) can withstand constitutional scrutiny, the Court must provide limiting instructions informed by *Morison*, *Rosen*, and the leading constitutional scholars commenting on the espionage statutes. At this time, Mr. Drake asks in particular for instructions regarding the vague phrase “relating to the national defense” and the term “willfully.”¹⁶

¹⁶ These are not the only elements of the offense. The Court also will have to instruct the jury on the meaning of “having unauthorized possession of, access to, or control over any document.” Mr. Drake intends to offer additional proposed jury instructions on this and other

A. Relating to the National Defense

When defining “relating to the national defense,” the Court should instruct the jury that the government must prove beyond a reasonable doubt that the documents contain information that, if disclosed, is potentially damaging to the United States. *See Morison*, 844 F.2d at 1071. The government must prove beyond a reasonable doubt that the documents at issue must be the sort that, if disclosed, would have a reasonable and direct chance of damaging national security, not a strained or distant likelihood. *See Gorin*, 312 U.S. at 31. The government must prove that the documents contain information that, if disclosed, would “imperil the environment of physical security which a functioning democracy requires.” *Morison*, 844 F.2d at 1082 (Wilkinson, J., concurring).

Additional instructions regarding this phrase are necessary here because, unlike *Morison*, this prosecution strikes at the heart of the First Amendment. Because this case raises such substantial First Amendment concerns, the jury instructions must include guidance from First Amendment cases as well. Therefore, the Court should instruct the jury that the government must prove, beyond a reasonable doubt, that “potentially damaging to the United States” means that disclosure of the information would be likely to cause imminent serious injury to the United States. *See New York Times*, 403 U.S. at 726-27 (Brennan, J., concurring); Nimmer, *Free Speech*, 26 Stan. L. Rev. at 331-32. The government must prove that the harm is serious, inevitable, and directly linked to the retention of the documents. *See New York Times*, 403 U.S. at 726-27 (Brennan, J., concurring).

B. Relating to the National Defense – Closely Held

When defining the phrase “relating to the national defense,” the Court should further instruct

trial-related issues as this case proceeds. The instructions included here, however, address Mr. Drake’s constitutional arguments raised in this motion.

the jury that the government must prove beyond a reasonable doubt that the government closely held the documents or information and that the defendant knew the documents or information was closely held. At a minimum, this means that the government must prove that the documents were classified. But the government must also prove beyond a reasonable doubt that the information was not otherwise available to the public. And the government must still prove, even if a document is classified, that the document is in fact potentially damaging to the security of the United States. *See Morison*, 844 F.2d at 1086 (Phillips, J., concurring); *Rosen*, 445 F. Supp. 2d at 624-25. That means that not every document that is classified constitutes a document relating to the national defense.

C. *Mens Rea*

A standard specific intent instruction would not be sufficient to satisfy the *mens rea* requirements under this statute. *See Rosen*, 445 F. Supp. 2d at 625-26. The term “willfully” should have three components that must be proven. First, the Court should instruct the jury that the government must prove beyond a reasonable doubt that Thomas Drake specifically intended to violate 18 U.S.C. § 793(e), and that he acted with a bad or underhanded purpose, not by an honest mistake. *See Morison*, 844 F.2d at 1071. Second, the Court should instruct the jury that the government must prove beyond a reasonable doubt that Mr. Drake knew that information contained in the documents related to the national defense, *i.e.*, that if disclosed, that information would harm national security. *See Rosen*, 445 F. Supp. 2d at 626 (citing *Morison*). Finally, the jury should be instructed that the government must prove beyond a reasonable doubt that Mr. Drake knew that the information contained in the documents was closely held. In addition to these instructions on “willfully,” the Court also should instruct the jury that the government must prove that Mr. Drake had “reason to believe [the information in the documents] . . . could be used to the injury of the

United States or to the advantage of any foreign nation.” *Id.* That additional scienter requirement is necessary in this case. If the government cannot prove beyond a reasonable doubt these *mens rea* requirements, then the jury must acquit Mr. Drake.

CONCLUSION

Section 793(e) is a statute of alarming breadth and little definition. Courts have repeatedly tried to limit its scope, acknowledging that without any limitations, the statute is unenforceable. But each judicial interpretation differs from the one before – no clear consensus has arisen as the meaning or limitation of the elements and terms in the statute. Moreover, the statute proscribes core political speech. Although the government has an interest in protecting national security, the statute is not narrowly tailored to that goal. This prosecution demonstrates how the reach of the statute is likely to exceed constitutional bounds and also highlights the importance of the pro-speech interests at stake. This Court should therefore dismiss Counts One through Five both because 18 U.S.C. § is unconstitutionally vague as applied to Mr. Drake, but also because it is unconstitutionally overbroad.

Respectfully submitted,

/s/

JAMES WYDA, #25298
Federal Public Defender
DEBORAH L. BOARDMAN, #28655
Assistant Federal Public Defender
MEGHAN SKELTON
Staff Attorney
Office of the Federal Public Defender
100 South Charles Street
Tower II, Ninth Floor
Baltimore, Maryland 21201
Phone: 410-962-3962
Fax: 410-962-0872
Email: Jim_Wyda@fd.org
Deborah_Boardman@fd.org
Meghan_Skelton@fd.org

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND**

UNITED STATES OF AMERICA

*

vs.

*

Case No. 1:10-cr-0181-RDB

THOMAS ANDREWS DRAKE

*

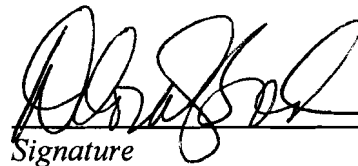
NOTICE OF FILING OF LENGTHY EXHIBIT

Exhibit A, which is an attachment to Defendant's Motion to Dismiss Counts 1-5

exists only in paper format. It will be filed with the Clerk's Office in paper format.

I certify that within 24 hours of the filing of this Notice, I will file and serve paper copies of the document identified above.

February 25, 2011
Date


Signature

Deborah L. Boardman 28655
Printed Name *Bar Number*

100 S. Charles Street, Tower II, Ninth Floor
Address

Baltimore, Maryland 21201
City/State/Zip

(410) 962-3962 (410) 962-0872
Phone No. *Fax No.*

THE ESPIONAGE ACT AND THE LEGAL AND CONSTITUTIONAL ISSUES RAISED BY WIKILEAKS
Hearing Before the House Committee on the Judiciary
Thursday, December 16, 2010

Prepared Statement of Stephen I. Vladeck

Professor of Law, American University Washington College of Law

Chairman Conyers, Ranking Member Smith, and distinguished members of the Committee:

Testifying before the House Permanent Select Committee on Intelligence in 1979, Anthony Lapham—then the General Counsel of the CIA—described the uncertainty surrounding the scope of the Espionage Act of 1917 as “the worst of both worlds.” As he explained,

On the one hand the laws stand idle and are not enforced at least in part because their meaning is so obscure, and on the other hand it is likely that the very obscurity of these laws serves to deter perfectly legitimate expression and debate by persons who must be as unsure of their liabilities as I am unsure of their obligations.

Whatever one’s views of WikiLeaks as an organization, of Julian Assange as an individual, or of public disclosures of classified information more generally, recent events have driven home Lapham’s central critique—that the uncertainty surrounding this 93-year-old statute benefits no one, and leaves too many questions unanswered about who may be held liable, and under what circumstances, for what types of conduct.

In my testimony today, I’d like to briefly identify five distinct ways in which the Espionage Act as currently written creates problematic uncertainty, and then, time permitting, suggest potential means of redressing these defects. I in no way mean to suggest that these five issues are the only problems with the current regime. Indeed, it is likely also worth addressing whether the Act should even apply to offenses committed by non-citizens outside the territorial United States. But looking forward, these five flaws are in my view the most significant problems, especially in the context of the recent disclosures by WikiLeaks.

First, as its title suggests, the Espionage Act of 1917 was designed and intended to deal with classic acts of espionage, which *Black’s Law Dictionary* defines as “The practice of using spies to collect information about what another

government or company is doing or plans to do.” As such, the plain text of the Act fails to require a specific intent either to harm the national security of the United States or to benefit a foreign power. Instead, the Act requires only that the defendant know or have “reason to believe” that the wrongfully obtained or disclosed “national defense information” is to be used to the injury of the United States, or to the advantage of any foreign nation. No separate statute deals with the specific—and, in my view, distinct—offense of disclosing national defense information in non-espionage cases. Thus, the government has traditionally been forced to shoehorn into the Espionage Act three distinct classes of cases that raise three distinct sets of issues: classic espionage; leaking; and the retention or redistribution of national defense information by private citizens. Again, whatever one’s views of the merits, I very much doubt that the Congress that drafted the statute in the midst of the First World War meant for it to cover each of those categories, let alone to cover them equally.

Second, the Espionage Act does not focus solely on the initial party who wrongfully discloses national defense information, but applies, in its terms, to *anyone* who knowingly disseminates, distributes, or even *retains* national defense information without immediately returning the material to the government officer authorized to possess it. In other words, the text of the Act draws no distinction between the leaker, the recipient of the leak, or the 100th person to redistribute, retransmit, or even *retain* the national defense information that, by that point, is already in the public domain. So long as the putative defendant knows or has reason to believe that their conduct is unlawful, they are violating the Act’s plain language, regardless of their specific intent and notwithstanding the very real fact that, by that point, the proverbial cat is long-since out of the bag. Whether one is a journalist, a blogger, a professor, or any other interested person is irrelevant for purposes of the statute. Indeed, this defect is part of why so much attention has been paid as of late to the potential liability of the press—so far as the plain text of the Act is concerned, one is hard-pressed to see a significant distinction between disclosures by WikiLeaks and the re-publication thereof by major media outlets. To be sure, the First Amendment may have a role to play there, as the Supreme Court’s 2001 decision in the *Bartnicki* case and the recent *AIPAC* litigation suggest, but I’ll come back to that in a moment. At the very least, one is forced to conclude that the Espionage Act leaves very much unclear whether there is *any* limit as to how far downstream its proscriptions apply.

Third, and related, courts struggling with these first two defects have reached a series of disparate conclusions as to the requisite *mens rea* that

individuals must have to violate the Act. Thus, and largely to obviate First Amendment concerns, Judge Ellis in the *AIPAC* case read into 18 U.S.C. § 793(e) a second *mens rea*. As he explained, whereas the statute’s “willfulness” requirement obligates the government to prove that defendants know that disclosing classified documents could threaten national security, and that it was illegal, it leaves open the possibility that defendants could be convicted for these acts despite some salutary motive. By contrast, the “reason to believe” requirement that accompanies disclosures of *information* (as distinct from “documents”), requires the government to demonstrate the likelihood of defendant’s bad faith *purpose* to either harm the United States or to aid a foreign government.

Whether or not one can meaningfully distinguish between the disclosure of “documents” and the disclosure of “information” in the digital age, it is clear at the very least that nothing in the text of the statute speaks to the defendant’s bad faith. Nor is there precedent for the proposition that “willfulness,” which the Espionage Act *does* require, is even remotely akin to “bad faith.” Instead, undeniable but poorly articulated constitutional concerns have compelled courts to read into the statute requirements that aren’t supported by its language. And in the *AIPAC* case, this very holding may well have been the impetus for the government’s decision to drop the prosecution. To be sure, a motive requirement may well separate the conduct of individuals like Julian Assange from the actions of media outlets like the *New York Times*, but if the harm that the law means to prevent is the disclosure of *any* information damaging to our national security, one is hard-pressed to see why the discloser’s motive should matter.

Fourth, the potentially sweeping nature of the Espionage Act as currently written may inadvertently interfere with federal whistleblower laws. For example, the Federal Whistleblower Protection Act (“WPA”) protects the public disclosure of “a violation of any law, rule, or regulation” only “if such disclosure is not specifically prohibited by law and if such information is not specifically required by Executive order to be kept secret in the interest of national defense or the conduct of foreign affairs.” And similar language appears in most other federal whistleblower protection statutes.

To be sure, the WPA, the Intelligence Community Whistleblower Protection Act, and the Military Whistleblower Protection Act all authorize the putative whistleblower to report to cleared government personnel in national security cases. And yet, there is no specific reference in any of these statutes to the Espionage Act, or to the very real possibility that those who receive the disclosed information, even

if they are “entitled to receive it” for purposes of the Espionage Act, might still fall within the ambit of 18 U.S.C. § 793(d), which prohibits the willful *retention* of national defense information. Superficially, one easy fix to the whistleblower statutes would be amendments that made clear that the individuals to whom disclosures are made under those statutes are “entitled to receive” such information under the Espionage Act. But Congress might also consider a more general proviso exempting protected disclosures from the Espionage Act—and other federal criminal laws—altogether.

Fifth, the Espionage Act does not deal in any way with the elephant in the room—situations where individuals disclose classified information that should never have been classified in the first place, including information about unlawful governmental programs and activities. Most significantly, every court to consider the issue has rejected the availability of an “improper classification” defense—a claim by the defendant that he cannot be prosecuted because the information he unlawfully disclosed was in fact unlawfully classified. If true, of course, such a defense would presumably render the underlying disclosure legal. It’s entirely understandable that the Espionage Act nowhere refers to “classification,” since our modern classification regime postdates the Act by over 30 years. Nevertheless, given the well-documented concerns today over the overclassification of sensitive governmental information, the absence of such a defense—or, more generally, of any specific reference to classification—is yet another reason why the Espionage Act’s potential sweep is so unclear. Even where it is objectively clear that the disclosed information was erroneously classified in the first place, the individual who discloses the information (and perhaps the individual who receives the disclosure) might (and I emphasize *might*) still be liable.

To whatever extent the five problems I have just outlined have always been present, it cannot be gainsaid that recent developments have brought them into sharp relief. To be sure, most of these problems have remained beneath the surface historically thanks to the careful administration of the Espionage Act by the Justice Department, including by my colleague Mr. Wainstein. Indeed, the *AIPAC* case remains the only example in the Espionage Act’s history of the government bringing a prosecution of someone *other than* the initial spy/leaker/thief. But as Chief Justice Roberts emphasized earlier this year, the Supreme Court “would not uphold an unconstitutional statute merely because the Government promised to use it responsibly.”

What, then, is to be done? Perhaps unsurprisingly in light of my observations above, I would recommend three distinct sets of changes to the current scope and structure of the Espionage Act:

- (1) Introduce a clear and precise specific intent requirement that constrains the scope of the Espionage Act to cases where the defendant specifically intends the disclosure to cause harm to the national security of the United States and/or to benefit a foreign power.
- (2) Create a separate, lesser offense for unauthorized disclosure and retention of classified information, and specifically provide either that such a prohibition covers or does *not* cover the public re-distribution of such information, including by the press. If the proscription *does* include re-transmission, my own view is that the First Amendment requires the availability of affirmative defenses that the disclosure was in good faith; that the information was improperly classified; that the information was already in the public domain; and/or that the public good resulting from the disclosure outweighs the potential harm to national security. Even still, there may be some applications of this provision that would violate the First Amendment, but at least the stakes would be clearer up front to all relevant actors.
- (3) Include in both the Espionage Act and any new unauthorized disclosure statute an express exemption for any disclosure that is covered by an applicable federal whistleblower statute.

But whatever path you and your colleagues choose to pursue, Mr. Chairman, the uncertainty surrounding the Act's applicability in the present context impels action in one direction or another. It's been nearly four decades since a pair of Columbia Law School professors—Hal Edgar and Benno Schmidt—lamented that, “the longer we looked [at the Espionage Act], the less we saw.” Instead, as they observed, “we have lived since World War I in a state of benign indeterminacy about the rules of law governing defense secrets.” If anything, such benign indeterminacy has only become more pronounced in the 40 years since—and, if recent events are any indication, increasingly less benign.

Thank you very much for the opportunity to testify before the Committee today. I look forward to your questions.

THE ESPIONAGE ACT: A LOOK BACK AND A LOOK FORWARD

Hearing Before the Senate Committee on the Judiciary

Subcommittee on Terrorism and Homeland Security

Wednesday, May 12, 2010

Written Testimony of Stephen I. Vladeck

Professor of Law, American University Washington College of Law

Mr. Chairman, Ranking Member Kyl, and distinguished members of the Subcommittee:

Thank you for inviting me to testify today on such an important—but often neglected—topic. I suspect that we all have common cause when it comes to the need for harsh criminal sanctions for those who commit acts of espionage against the United States, and the Espionage Act of 1917 and its related statutes are vital in ensuring that the unauthorized disclosure of our national security secrets is not just prohibited, but severely punished.

And yet, as significant as the Espionage Act is (and has been), it is also marked by profound and frustrating ambiguities and internal inconsistencies. Attempting to distill clear principles from the state of the federal espionage laws in 1973, a pair of Columbia Law School professors—Hal Edgar and Benno Schmidt—lamented that, “the longer we looked, the less we saw.” Instead, as they observed, “we have lived since World War I in a state of benign indeterminacy about the rules of law governing defense secrets.”¹ If anything, such benign indeterminacy has only become more pronounced in the four decades since—and, according to some, increasingly less benign.

I. Statutory Background²

a. The Espionage Act

1. See Harold Edgar & Benno C. Schmidt, Jr., *The Espionage Statutes and Publication of Defense Information*, 73 COLUM. L. REV. 929 (1973).

2. This background discussion is taken from Stephen I. Vladeck, *Inchoate Liability and the Espionage Act: The Statutory Framework and the Freedom of the Press*, 1 HARV. L. & POL'Y REV. 219, 221–31 (2007).

From the Sedition Act of 1798 (which expired in 1801) through the outbreak of the First World War, there was virtually no federal legislation prohibiting seditious expression. Indeed, there were no general federal laws prohibiting the dissemination or publication of almost any information potentially harmful to the national defense. Contemporaneously with the United States's entry into the war, however, Congress enacted the Espionage Act of 1917, which, except for the amendments discussed below, remains on the books largely in its original form today at 18 U.S.C. §§ 793–99. Drafted principally by then-Assistant Attorney General Charles Warren, the Act includes a number of seemingly overlapping and often ambiguous provisions.

Current 18 U.S.C. § 793(a), which derives from section 1(a) of the Espionage Act, prohibits the obtaining of information concerning a series of national defense installations—places—“with intent or reason to believe that the information is to be used to the injury of the United States, or to the advantage of any foreign nation.” Similarly, § 793(b) prohibits individuals with “like intent or reason to believe” from copying, taking, making, or obtaining “any sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, document, writing, or note of anything connected with the national defense.” Although an early legal challenge argued that the requirement that the information at issue be “connected with the national defense” was unconstitutionally vague, the Supreme Court read a scienter requirement into the statute (and, so construed, upheld it) in *Gorin v. United States* in 1941.³

Section 793(c) is, in important ways, far broader. The descendant of section 1(c) of the original Espionage Act, this provision creates criminal liability for any individual who “receives or obtains or agrees or attempts to receive or obtain from any person, or from any

3. See 312 U.S. 19, 27–28 (1941) (“The obvious delimiting words in the statute are those requiring ‘intent or reason to believe that the information to be obtained is to be used to the injury of the United States, or to the advantage of any foreign nation.’”).

source whatever” various material related to the national defense, so long as the individual “know[s] or ha[s] reason to believe, at the time he receives or obtains [the information] ... that it has been or will be obtained, taken, made, or disposed of by any person contrary to the provisions of [the Espionage Act].” Thus, whereas §§ 793(a) and 793(b) prohibit the collection of secret information relating to the national defense, § 793(c) prohibits the receipt of such information, or even attempts at receipt thereof, so long as the recipient does or should have knowledge that the source, in obtaining the information, violated some other provision of the Espionage Act.

In addition, whereas §§ 793(d) and 793(f) prohibit the dissemination of national security information that is in the lawful possession of the individual who disseminates it (§ 793(d) prohibits willful communication; § 793(f) prohibits negligence), § 793(e)—which, like § 793(d) and 793(f), derives from section 1(d) of the Espionage Act—prohibits the same by an individual who has unauthorized possession of the information at issue.

Thus, in sweeping language, § 793(e) prohibits individuals from willfully communicating—or attempting to communicate—to any person not entitled to receive it:

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.

Section 793(e) goes one important step further, however, for it also prohibits the retention of such information and the concomitant failure to deliver such information “to the officer or employee of the United States entitled to receive it.” Section 793(e) therefore appears to have a far more relaxed intent requirement than § 793(a) and 793(b). The provision does not require specific intent so long as the communication or retention of classified information is “willful,” a point on which I will elaborate below.

One of the important questions that has arisen with regard to § 793(e) is whether, and to what extent, it might apply to the press. Many have argued against the applicability of § 793(e) to the press because of the absence of an express reference to the “publication” of such secret national security information. In contrast, three separate provisions of the Espionage Act *do* expressly prohibit the *publication* of particular national defense information:

First, § 794(b) applies to “[w]hoever, in time of war, with intent that the same shall be communicated to the enemy, collects, records, publishes, or communicates ... [the disposition of armed forces] or any other information relating to the public defense, which might be useful to the enemy.” Although the provision might appear to turn on whether it is a “time of war,” a subsequently enacted provision—§ 798A—expands § 794(b) to apply so long as various national emergencies remain in place, a condition that remains satisfied today. Second, § 797 applies to whoever “reproduces, publishes, sells, or gives away” photographs of specified defense installations, unless the photographs were properly censored.

Third, § 798(a), which generally relates to cryptography and was passed in 1950 at least largely in response to the *Chicago Tribune* incident from World War II,⁴ applies to whoever “communicates, furnishes, transmits, or otherwise makes available ... or publishes” various prohibited materials, including “classified information ... concerning the communication intelligence activities of the United States or any foreign government.” Section 798(b) defines “classified information” as “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.” Whether the

4. Shortly after the Battle of Midway, the *Chicago Tribune* ran a series of articles suggesting that the U.S. Navy had prevailed largely because it had prior warning of the location of the Japanese attack. Concerned that Japanese intelligence would correctly surmise that the Americans had broken Japanese naval codes, the government initiated criminal proceedings against the *Tribune*. Fearful that the prosecution would itself tip off the Japanese, though, the United States dropped the case. See Jeffery A. Smith, *Prior Restraint: Original Intentions and Modern Interpretations*, 28 WM. & MARY L. REV. 439, 467 (1987).

specific references to publication in these three sections exclude the applicability of other provisions of the statute to the press is an issue to which I shall return shortly.

One other noteworthy provision of the Espionage Act is 18 U.S.C. § 794(a), which applies to “[w]hoever, with intent or reason to believe that it is to be used to the injury of the United States or to the advantage of a foreign nation, communicates, delivers, or transmits ... to any foreign government, or to any faction or party or military or naval force within a foreign country, ... any document, ... [other physical items], or information relating to the national defense.” To similar effect is 50 U.S.C. § 783, enacted as part of the 1950 amendments to the Espionage Act. Section 783 also prohibits the communication of classified information by an “officer or employee of the United States” to agents or representatives of foreign governments (even though such individuals were presumably already subject to liability under § 794(a)).

Finally, it is critical to note that the Espionage Act also contains two independent conspiracy provisions. Pursuant to § 793(g), “[i]f two or more persons conspire to violate any of the foregoing provisions of this section, and one or more of such persons do any act to effect the object of the conspiracy, each of the parties to such conspiracy shall be subject to the punishment provided for the offense which is the object of such conspiracy.” Section 794(c) is to similar effect.

b. Espionage-Related Statutes

The Espionage Act, while important, is merely one subset of a much larger range of statutes pertaining to the unlawful disclosure of national security secrets. First, and perhaps most important, is 18 U.S.C. § 641, one of the statutes at issue (along with § 793(d) and 793(e)) in the famous case of *United States v. Morison*.⁵ Originally enacted in 1875, § 641 applies to:

5. 844 F.2d 1057 (4th Cir. 1988).

Whoever ... knowingly converts to his use or the use of another, or without authority, sells, conveys or disposes of any record, voucher, money, or thing of value of the United States or of any department or agency thereof ...; or

Whoever receives, conceals, or retains the same with intent to convert it to his use or gain, knowing it to have been embezzled, stolen, purloined or converted

Thus, § 641, in general terms, prohibits the conversion of any “thing of value” to the U.S. government, and also prohibits the knowing receipt of the same, “with intent to convert it to his use or gain.”

Relying on § 641, the government prosecuted Samuel Morison for transmitting photographs of a new Soviet aircraft carrier to *Jane’s Defence Weekly*, an English publisher of defense information. As the Fourth Circuit explained:

The defendant would deny the application of [§ 641] to his theft because he says that he did not steal the material “for private, covert use in illegal enterprises” but in order to give it to the press for public dissemination and information The mere fact that one has stolen a document in order that he may deliver it to the press, whether for money or for other personal gain, will not immunize him from responsibility for his criminal act.

Considered in conjunction with the concerns noted above, the potential liability under § 641 may be just as broad, if not broader, than the liability under §§ 793(d) and 793(e). As Judge Winter worried in *United States v. Truong Dinh Hung*:

[B]ecause the statute was not drawn with the unauthorized disclosure of government information in mind, § 641 is not carefully crafted to specify exactly when disclosure of government information is illegal This ambiguity is particularly disturbing because government information forms the basis of much of the discussion of public issues and, as a result, the unclear language of the statute threatens to impinge upon rights protected by the first amendment. Under § 641 as it is written, . . . upper level government employees might use their discretion in an arbitrary fashion to prevent the disclosure of government information; and government employees, newspapers, and others could not be confident in many circumstances that the disclosure of a particular piece of government information was “authorized” within the meaning of § 641.⁶

6. 629 F.2d 908, 924–25 (4th Cir. 1980).

Also relevant to any discussion of governmental secrecy are 18 U.S.C. §§ 952 and 1924. Enacted in 1933, § 952 relates specifically to diplomatic codes and correspondence, and applies to government employees who, without authorization, publish or provide to a third-party diplomatic codes, or diplomatic correspondence “obtained while in the process of transmission between any foreign government and its diplomatic mission in the United States.” A fair reading of the statute is that it prohibits the publication by the government employee, and not by an independent third-party, but the disclosure by non-governmental employees of encrypted communications between the United States and foreign governments or its overseas missions could still plausibly be said to fall within that provision’s purview.

Similarly, 18 U.S.C. § 1924, enacted in 1994, prohibits the unauthorized removal and retention of classified documents or material. It applies to:

Whoever, being an officer, employee, contractor, or consultant of the United States, and, by virtue of his office, employment, position, or contract, becomes possessed of documents or materials containing classified information of the United States, [who] knowingly removes such documents or materials without authority and with the intent to retain such documents or materials at an unauthorized location.

Three additional statutes, which regulate specific types of secret information, are also relevant to today’s discussion. First among these is the Atomic Energy Act of 1954, 42 U.S.C. §§ 2011 to 2296b-7. Sections 2274, 2275, and 2277 thereof prohibit the communication, receipt, and disclosure, respectively, of “Restricted Data,” which is defined as “all data concerning (1) design, manufacture, or utilization of atomic weapons; (2) the production of special nuclear material; or (3) the use of special nuclear material in the production of energy, but shall not include data declassified or removed from the Restricted Data category pursuant to section 2162 of this title.” In the *Progressive* case, in which the U.S. government successfully enjoined

the publication of an article titled “The H-Bomb Secret: How We Got It, Why We’re Telling It,” it was the potential violation of § 2274(b) that formed the basis for the injunction.⁷

A very different statute, and one arguably of more relevance today (at least in light of the Valerie Plame affair) is the Intelligence Identities Protection Act of 1982, 50 U.S.C. §§ 421–426. Specifically, § 421 prohibits the disclosure of information relating to the identity of covert agents. Whereas § 421(a) and 421(b) prohibit the disclosure of such information by individuals authorized to have access to classified information identifying the agent, § 421(c) applies to anyone who “discloses any information that identifies an individual as a covert agent to any individual not authorized to receive classified information, knowing that the information disclosed so identifies such individual and that the United States is taking affirmative measures to conceal such individual's classified intelligence relationship to the United States.” The individual must “intend[] to identify and expose covert agents and [have] reason to believe that such activities would impair or impede the foreign intelligence activities of the United States.” Importantly, though, § 421(c) “does not predicate liability on either access to or publication of classified information.”

Finally, the Invention Secrecy Act of 1951, 35 U.S.C. §§ 181–188, protects the disclosure of information relating to patents under “secrecy” orders. The statutory punishment, however, for disclosure of information relating to a patent under a secrecy order is forfeiture of the patent. No criminal liability appears to attach to such disclosures.

II. The Espionage Act’s Key Ambiguities

For starters, it should be clear from the above survey that the Espionage Act and related statutes are difficult to parse, and often seem targeted at distinct (and perhaps

7. See *United States v. The Progressive, Inc.*, 467 F. Supp. 990, 993–96 (W.D. Wis.), *appeal dismissed*, 610 F.2d 819 (7th Cir. 1979).

contradictory) goals. Although there are a number of ambiguities raised by the language of these provisions in their current form, four specific incongruities are particularly troubling.

The first—and most systematic—defect concerns the statute’s ambiguous scope, by which I mean whether it applies to anything beyond classic spying. Enacted specifically to punish “espionage,” which *Black’s Law Dictionary* defines as “The practice of using spies to collect information about what another government or company is doing or plans to do,” the plain text of the Act fails to require a specific intent either to harm the national security of the United States or to benefit a foreign power. Instead, the Act requires only that the defendant know or have “reason to believe” that the wrongfully obtained or disclosed “national defense information” is to be used to the injury of the United States, or to the advantage of any foreign nation.

As a result of this lax *mens rea* requirement, the Espionage Act could be applied as currently written to prosecute government employees or private citizens in cases bearing little resemblance to classic espionage. Such cases could include situations in which a government employee seeks to reveal the details of an unlawful secret program, or to bring to the attention of the relevant Inspector General or oversight officer the existence of information that was wrongfully classified; and cases in which a private citizen comes into the possession of classified information with no desire to harm our national security. In each of these circumstances, an informed citizen would certainly “have reason to believe” that the relevant information, if publicly disclosed, could cause injury to the national security of the United States or benefit a foreign power. That knowledge, though, need not (and often will not) bear any relationship to the defendant’s actual motive.

Moreover, these concerns are hardly academic, as we’ve seen in the recent *AIPAC* case. There, the government prosecuted Steven Rosen and Keith Weissman, lobbyists for the

American Israel Public Affairs Committee, for receiving classified information about the Middle East, Iran, and terrorism from a Defense Department analyst before passing that information on to a journalist and an Israeli diplomat. That case involved perhaps the broadest provision of the Espionage Act, 18 U.S.C. § 793(e), which prohibits anyone in the unauthorized possession of national security information from “willfully communicat[ing], deliver[ing], transmit[ing] or caus[ing] to be communicated, delivered, or transmitted . . . [such information] to any person not entitled to receive it, or willfully retain[ing] the same and fail[ing] to deliver it to the officer or employee of the United States entitled to receive it.” In upholding the first-ever use of § 793(e) in a case against non-governmental employees, the district court noted that the text of the statute “leaves open the possibility that defendants could be convicted for these acts despite some salutary motive.”

The second key defect in the Espionage Act, which is related to its ambiguous scope, is the question of how, if at all, it applies to whistleblowers. For example, the Federal Whistleblower Protection Act (“WPA”), protects the public disclosure of “a violation of any law, rule, or regulation” only “if such disclosure is not specifically prohibited by law and if such information is not specifically required by Executive order to be kept secret in the interest of national defense or the conduct of foreign affairs.”⁸ Similar language appears in most other federal whistleblower protection statutes.

To be sure, the WPA, the Intelligence Community Whistleblower Protection Act, and the Military Whistleblower Protection Act all authorize the putative whistleblower to report to cleared government personnel in national security cases. And yet, there is no specific reference in any of these statutes to the Espionage Act, or to the very real possibility that those who receive the disclosed information, even if they are “entitled to receive it” for purposes of the

8. 5 U.S.C. § 1213(a).

Espionage Act (which itself is hardly clear), might still fall within the ambit of 18 U.S.C. § 793(d), which prohibits the willful retention of national defense information. Superficially, one easy fix to the whistleblower statutes would be amendments that made clear that the individuals to whom disclosures are supposed to be made under those statutes are “entitled to receive” such information under the Espionage Act. But Congress might also consider a more general proviso exempting protected disclosures from the Espionage Act altogether.

Another important (and related) ambiguity with the Espionage Act is whether and to what extent it might apply to the press. As with the whistleblower example I just described, a reporter to whom a government employee leaks classified information could theoretically be prosecuted merely for retaining that information, and could almost certainly be prosecuted for disclosing that information (including by publishing it). And yet, it seems clear from the legislative history surrounding the Espionage Act that § 793(e) was never meant to apply to the press; indeed, as noted above, three other provisions of the Espionage Act specifically prohibit publication of national defense information, and another, broader limitation on the retention of national security information by the press was specifically scrapped by Congress, suggesting that the Act is express in those few places where it specifically targets newsgathering.

Finally, the Espionage Act is also silent as to potential defenses to prosecution. Most significantly, every court to consider the issue has rejected the availability of an “improper classification” defense—a claim by the defendant that the information he unlawfully disclosed was in fact unlawfully classified.⁹ If true, of course, such a defense would presumably render the underlying disclosure legal. It’s entirely understandable that the Espionage Act nowhere refers to “classification,” since our modern classification regime postdates the Act by over 30

9. *See, e.g.*, *United States v. Boyce*, 594 F.2d 1246 (9th Cir. 1979); *see also Scarbeck v. United States*, 317 F.2d 546 (D.C. Cir. 1963).

years. Nevertheless, given the well-documented concerns today over the overclassification of sensitive governmental information, the absence of such a defense—or, more generally, of any specific reference to classification—is yet another reason why the Espionage Act’s potential sweep is so broad. Even where it is objectively clear that the disclosed information was erroneously classified in the first place, the individual who discloses the information (and perhaps the individual who receives the disclosure) might still be liable.

Although statutory ambiguity is hardly a vice in the abstract, in the specific context of the Espionage Act, these ambiguities have two distinct—and contradictory—effects. Testifying before Congress in 1979, Anthony Lapham, the General Counsel of the CIA, put it this way:

On the one hand the laws stand idle and are not enforced at least in part because their meaning is so obscure, and on the other hand it is likely that the very obscurity of these laws serves to deter perfectly legitimate expression and debate by persons who must be as unsure of their liabilities as I am unsure of their obligations.

And to whatever extent these problems have always been present, recent developments lend additional urgency to today’s endeavor. In addition to the *AIPAC* case I mentioned earlier, a report released just last week by the Heritage Foundation and the National Association of Criminal Defense Lawyers (strange bedfellows, to be sure) highlighted the growing concerns among courts and commentators alike over problems of vagueness and overbreadth in contemporary federal criminal laws, let alone an antiquated statute like the Espionage Act. And just last month, the Supreme Court in the crush-video decision reiterated its concern with congressional statutes that may chill constitutionally protected speech. As Chief Justice Roberts emphasized for an 8-1 majority, the Court “would not uphold an unconstitutional statute merely because the Government promised to use it responsibly.”

In short, then, although it is not my place to make specific recommendations to this Subcommittee with regard to how the Espionage Act might be updated, it seems clear that the

current state of the law is counterproductive regardless of the specific policy goals one might seek to pursue. As Judge Ellis observed in the *AIPAC* case,

The conclusion that the statute is constitutionally permissible does not reflect a judgment about whether Congress could strike a more appropriate balance between these competing interests, or whether a more carefully drawn statute could better serve both the national security and the value of public debate. . . . [Changes in the nature of threats to our national security over the last few decades] should suggest to even the most casual observer that the time is ripe for Congress to engage in a thorough review and revision of these provisions to ensure that they reflect both these changes, and contemporary views about the appropriate balance between our nation's security and our citizens' ability to engage in public debate about the United States' conduct in the society of nations.¹⁰

To that end, if Congress were ultimately to conclude that the Espionage Act should be limited to cases of classic espionage and perhaps other malicious disclosures of classified information, my suggestion would be to focus carefully on the *mens rea* in the statute, and to consider the adoption of something akin to a specific intent requirement—that the offender not just know that the disclosure would be harmful to our national security, but that he or she actually intend such harm. If Congress were ultimately to conclude that the Espionage Act should instead apply to all cases of legally unauthorized disclosures of classified information, then my view is that much of the current statutory language is superfluous and unnecessary, and that a far simpler prohibition, combined with clear indicia as to the provision's scope, would avoid the myriad vagueness and overbreadth issues that currently plague the statute. If, as a third way, Congress were to conclude that there should be separate penalties for unauthorized disclosures without an intent to harm our national security, then, once more, I think more precise statutory language is called for, with clearer definitions as to the classes of individuals to which each particular provision is intended to apply.

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

Either way, though, my own view is that Judge Ellis had it exactly right that time is ripe for congressional revisiting of this statutory scheme, and I thank the Subcommittee for taking up his call.