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 Background[2]

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[ting] 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 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.