

**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.