COMMITTEE ON THE JUDICIARY
U.S. HOUSE OF REPRESENTATIVES

Hearing on the Espionage Act and
the Legal And Constitutional Issues Raised by WikiLeaks

December 16, 2010

Written Statement of Abbe David Lowell
Partner, McDermott Will & Emery, LLP[1]

Chairman Conyers, Ranking Member Smith, and Members of the Committee on the Judiciary, thank you for inviting me to speak with you today about the Espionage Act of 1917 and the legal and constitutional issues raised by the distribution and publication of classified information by WikiLeaks and other entities.

A. Background With The Espionage Act

My involvement with the Espionage Act and its related statutes (e.g., the Classified Information Protection Act ["CIPA"]) stems from my time working in the Department of Justice as Special Assistant to the Attorney General (when CIPA was first drafted and enacted) and in my criminal defense practice. (I was one of the attorneys in the case charged in Alexandria, Virginia against the former lobbyists for the American-Israeli Public Affairs Committee ["AIPAC"], and I am currently representing a former Department of State analyst who was charged in the District of Columbia this past August under the Espionage Act for allegedly leaking information to the media.)

[1] These are the views of Mr. Lowell and not of the law firm that is named for identification purposes.

B. General Principles

It makes sense to start with the obvious and important – this nation needs a strong law that makes criminal and treats as seriously as possible anyone who spies on our country; we need to address just as seriously a purposeful disclosure of national defense information ("NDI") with the intent to injure the United States or assist an enemy of our country; and there has to be a prohibition for the mishandling of properly-classified information (which may or may not be NDI).

To address these issues, the differences in these categories – spying (or real espionage), disclosure of national defense information (NDI), and mishandling of classified information – should be set out in separate provisions of the law, each that clearly defines the offense it seeks to address and each with penalties appropriate for the conduct involved. One significant problem with the Act, currently, is that its antiquated structure still lumps or can lump these three separate forms of violation in the same sections of the statute. This neither serves justice well when it seeks to address the most egregious conduct (e.g., a government official who, for money or misplaced loyalty, provides NDI to an adversary) nor promotes fairness when it is applied to lesser offenses (e.g., a government official including classified information in an oral conversation as part of his/her regular work when talking to someone outside of government).

C. The Problem Of Over-Classification

One problem with any law that addresses the improper disclosure of classified information, of course, is the over-classification of information. I realize this is not an issue the Committee is specifically addressing, but it is an important consideration when a law

criminalizes disclosure of such material. As one saying goes: "when everything is classified, nothing really is classified." The government's former "classification czar," J. William Leonard, testified to Congress, "[i]t is no secret that the government classifies too much information."[2] During that same hearing, the Department of Defense's Undersecretary for Intelligence, Carol Haave, echoed this point.[3] When asked to assess the rate of overclassification, both Leonard and Haave stated that probably about half of all classified information is overclassified.[4] Some agencies even classify newspaper articles and other public domain materials.

Any law would work best if applied to a system that carefully distinguished between that information that should be closely held and that which may be confidential from a policy or political point of view, but not from the perspective of national security. As we can now read in the material released by WikiLeaks, there is material that is classified presumably because it may be embarrassing to someone (a diplomat's opinion about the private life of a foreign leader) rather than something that is classified because it readily relates to national security (the plan to take military action if a foreign leader provokes a confrontation). Too often, government officials during their day's work find it easier to classify information or classify it at a higher level than necessary because it requires more effort and consideration to do less. No one gets in

---

2 "Too Many Secrets: Overclassification as a Barrier to Critical Information Sharing," Hearings Before Subcomm. On Nat'l Security, Emerging Threats and Int'l Relations, Comm. On Gov't Reform, U.S. House of Representatives, August 24, 2004 ("Too Many Secrets"), Tr. at 23.

3 *Id.* at 82 ("I do believe that we overclassify information.").

4 *See id.* at 82-83.

trouble for classifying something that should be unclassified, but people get in trouble for the opposite. Congress should keep this in mind when legislating a criminal law for the disclosure of what might turn out to have been improperly classified in the first place.

D. The Current Espionage Act Provisions

After WWII, there was a proposal to enact legislation prohibiting the disclosure of any classified information.[5] Congress rejected this approach, and instead, in 1950, passed one section of the current Espionage Act (18 U.S.C. §798). Again with reference to the way the world worked 50 years ago, Section 798 criminalizes the disclosure of four very specific types of classified information, primarily relating to the government's cryptographic systems and communication intelligence activities. This section of the law makes it a crime to "knowingly and willfully communicate[], furnish[], transmit[], or otherwise make[] available to an unauthorized person, or publish[], or use[]" the information "in any manner prejudicial to the safety or interest of the United States or for the benefit of any foreign government to the detriment of the United States[.]"

This section is far from clear. For example, Section 798 defines "classified information" as information that was made confidential "for reasons of national security."[6] So this raises very

---

[5] *See* Report of the Joint Committee on the Investigation of the Pearl Harbor Attack, S. Doc. No. 244, 79th CONG., 2d Sess. at 252-531 (1946).

[6] 18 U.S.C. § 798(b).

specifically the issue (and a possible defense) of whether something was improperly classified.[7]

The statute is ambiguous as to whether it requires a prosecutor to prove that each of the enumerated activities – such as communication or publication of the information – must be to the prejudice or detriment of the United States. One plausible reading of the statute, which two courts appear to have adopted, is that where the defendant is charged with communicating or publishing the information, the prosecutor need only has prove that the information was classified; by contrast, where the defendant is charged with "using" the information, a prosecutor must prove a risk of harm. This interpretation raises First Amendment concerns, because it lets a jury convict someone for publishing classified information without any evidence of potential harm to national security. And as a practical matter, it makes little sense to apply different standards to "communication," "publication," and "use," because digital technology and the Internet have significantly blurred, if not entirely erased, the lines between "communicating," "publishing," and "using" information.

Another section of the law (18 U.S.C. §793), that was used to charge the former AIPAC lobbyists, prohibits "willfully" disclosing "information relating to the national defense." This section may be even less clear than Section 798. First, the law does not actually make it illegal to disclose classified information. Instead, it talks about documents and information "relating to the national defense." This is a broad term that could refer not only to things like troop locations

---

[7] *See, e.g., United States v. Boyce*, 594 F.2d 1246 (9th Cir. 1979) *but see* S. Rep. No. 111, 81st Cong., 1st Sess., at 3 (1949)("The bill specifies that the classification must be in fact in the interests of national security")(emphasis added); H.R. Rep. No. 1895, 81st Cong., 2d Sess., at 3 (1950) (same).

and nuclear launch codes, but also to documents whose release would probably benefit the nation, such as proof of corruption in the awarding of armament contracts. Second, 2010 vocabulary is different than that used in 1917 – the term today is "national security" not "national defense," and it is unclear how the two concepts may differ. Third, the text of Section 793 treats national defense "documents" differently from national defense "information." As written, the law does not require prosecutors to prove that national defense "documents" pose a risk to the United States, and therefore raises many of the same First Amendment concerns that Section 798 does[8]. And fourth, while the statute does not distinguish between theft and mere receipt of classified information, journalists have and will continue to argue that the First Amendment requires this distinction.[9]

E. Questions Under The Current Law

What is primarily missing in the Act right now is clarity. The statute has been attacked often as vague and overbroad (this was done in the AIPAC lobbyists' case). Because of its breadth and language, it can be applied in a manner that infringes on proper First Amendment activity: discussions of foreign policy between government officials and private parties or proper newsgathering to expose government wrongdoing.

---

[8] The law even applies to a refusal to give back national defense information once a request has been made. How does that apply in the world of the Internet and electronic data?

[9] For example, the Supreme Court's decision in *Bartnicki v. Vopper*, 532 U.S. 514 (2001) held that it was unconstitutional to apply to the press a statute making it illegal to disclose illegally obtained information, where the information was of public concern and the press simply received the information but played no role in how it was obtained.

To save the law from constitutional attacks, courts have bent and twisted the Act's language to engraft various evidentiary requirements to conform it to both the First Amendment and Due Process Clause. Still it is a morass; let me just list some of the questions that the current statute and its language raise:

- Should portions of the statute (the portions used to address "leaks") be applied to non-government people, including those who receive the information covered as part of their First Amendment-protected activity and, if so, what additional safeguards are then required?

- To violate the espionage provision, does a person have to act to injure the United States or assist an enemy or a foreign country or all three or any? And how does one define the "reason to believe that the information is potentially damaging" provision that courts have imposed?

- How does one even measure "potentially damaging" to the national defense (e.g., if an item has a 1% chance of being damaging, is that enough?) and is it the information itself or the disclosure of the information that triggers that standard?

- Does the criminal intent (scienter) requirement mean that a person has to purposely intend to disclose what he or she knows is being kept confidential but also do so with the specific intent to injure our country or assist another? Especially in the First Amendment context, should not there be the higher requirement?

- When courts have ruled that the government has to prove a person acted with "bad faith," what does that mean?

- As the law requires that disclosures are made to people who are "not authorized" to receive it, how do government officials know, when they are talking to the media, the occasions when "leaks" are what their superiors want and have done themselves versus when they are violating the rules by speaking out of turn? How do those talking to government officials (for example the media) know that one leak is "authorized" and another is not?

- The law speaks of tangible things – maps, documents, etc. – and yet can it possibly be applied when government officials and others (including the media) just discuss things that they normally do as part of their jobs (and in those

conversations touch on information that is contained in a document or other tangible object somewhere)?

- If national defense information is more than information that is classified, how much more does it have to be? And when is a piece of information so "out there" that it is no longer closely held even if it is still contained in a classified document?

These are just some of the questions the current language raise and there are a legal pad of others.

F. The Case Of The Former AIPAC Lobbyists

The AIPAC lobbyist case is a good vehicle for the Committee to analyze the Act. In that case, for reasons that we still do not know, counter-intelligence and/or law enforcement agencies began following and investigating AIPAC employees in their dealings with U.S. government and Government of Israel officials. These AIPAC foreign policy experts were relied on by U.S. government officials for information and they, in turn, did their jobs of advising AIPAC and others in the community based on their government interactions. The AIPAC people did not have confidentiality agreements with the government, were not given security clearances to do their work, and were never told (except in a DOJ sting) that they should not be hearing what they were hearing. Nevertheless, not only were these two individuals investigated, they were charged with violating the Espionage Act. Before the actual charges were filed, in meetings with the Justice Department, government attorneys even raised the possibility that the two could be charged under the most severe section (i.e., spying) of the statute (18 U.S.C. § 794) for which the punishment included the death penalty.

So, in other words, the Act was applied to the following situation: (a) non-government officials, (b) who had no confidentiality agreements, (c) who received no tangible material and only talked with government officials, (d) who did not steal the information involved, (e) who did not sell the information involved, (f) who were doing the First Amendment-protected job they did for decades and believed they were helping (not hurting) the U.S.; and (g) who met only in public places and only during their real business hours and took other actions indicating they did not think what they were doing was improper.

G. The Current WikiLeaks Events

Now the world is focused on WikiLeaks and there is word that a grand jury in Alexandria, Virginia is considering the evidence. If the Espionage Act were used to bring charges against WikiLeaks or its founder, Julian Assange, this too would be unprecedented because it would be applying the law to a (a) non-government official, (b) who had no confidentiality agreement, (c) who did not steal the information, (d) who did not sell or pay for the information involved, (e) who was quite out front and not secretive about what he was doing, (f) who gave the U.S. notice and asked if the government wanted to make redactions to protect any information, and (g) in a context that can be argued to be newsgathering and dissemination protected by the First Amendment. If the Act applies to this disclosure, then why does it not apply as well to the articles written by *The New York Times* and other traditional media with the same disclosures? On its face, the Espionage Act does not distinguish between these two disclosures and would apply equally to both and to any even further dissemination of the same information.

H. Classified Information And The First Amendment

The mere fact that classified information is involved does not mean that the Constitution has no application. The First Amendment is intended to facilitate public discourse and collective decision-making about matters of public concern, particularly government affairs. Words and ideas are still words and ideas even if the Executive Branch deems them too dangerous to be disclosed to the public. As a result, in the AIPAC lobbyists' case, the federal district court judge rejected the prosecutors' categorical argument that when classified information is at issue, the First Amendment affords no protection whatsoever. There has never been a prosecution of a media organization under the Espionage Act, and the issue was a tangent to a few members of the Supreme Court that decided the Pentagon Papers case in 1971 (a case brought for a prior civil restraining order, not a criminal prosecution).

What the First Amendment does is to balance the societal interests in public discourse, on the one hand, and a genuine risk of harm, on the other.[10] When foreign policy information is made public, as was done by WikiLeaks and the traditional press, and as was done by *The New York Times* in the Pentagon Papers case, it almost certainly implicates the type of public discourse that the First Amendment is intended to protect. In addition, the fact that the information was made public could affect the assessment of the damage to national security. In a traditional case of selling secrets to a foreign power, our government may not know for years that classified information has made its way into the enemy's hands, and therefore we take no

[10] There is the well-known requirement in First Amendment cases, including those dealing with classified information to convince a jury, beyond a reasonable doubt, that the disclosures posed a clear and present danger to national security. *Hartzel v. United States*, 322 U.S. 680, 687 (1944).

steps to mitigate the damage of the disclosures. By contrast, when the revelations are as public as the WikiLeaks material has been, our government can at least be certain what exactly it is that our adversaries have learned.

Of course, the First Amendment would not and should not provide blanket immunity, for example, to a newspaper that tips off enemy forces by publishing a story that describes, in advance, a planned assault by the U.S. military on an Al Qaeda or Taliban stronghold. While such a news report might arguably provide some benefit to public understanding of our government, the imminent and likely risk of harm to American troops would far outweigh any such benefit, and that there would be no First Amendment protection for such a publication.

That the same section or sections of the Act can be used to prosecute discussions of pure foreign policy as in the AIPAC lobbyists context, the opinions of diplomats about the private life of world leaders as has occurred in WikiLeaks, and former FBI agent turned Russian spy Robert Hannsen demonstrates that the statute both sweeps too broadly and also does not properly address the real conduct it seeks to make criminal. The Act's breadth and vagueness can, intentionally or not, result in a powerful chill on the kinds of open government, freedom of the press, and transparency in proper foreign policy formulation that makes this country stronger. It does not serve proper national security or law enforcement interests to have this possibility of improper application of the Act to conduct that was not targeted in 1917 and has even less reason to be targeted today.

I. Recommendations For A New Law

Accordingly, Congress should revise the Act. It is almost 100 years old and was passed at a time and in an era that has little resemblance to the type of threats the county faces now or for the way information is disseminated today. Even so, the Act was criticized when it was passed and almost every decade later for issues similar to those being discussed now. Accordingly a newly formulated statute should:

1) carefully define espionage to prohibit the seeking or receipt of national defense information (NDI) with the intent to injure the U.S. or assist a foreign adversary; NDI has to be defined to mean: information that includes or relates to the country's national security, preparedness and homeland security in ways that do not include the normal conversations and exchanges about foreign policy that have existed since the country was founded;

2) define and appropriately punish a separate offense for the improper disclosure of NDI, similarly defined, when the purpose is not to injure the U.S. or assist a foreign adversary;

3) define and properly punish a separate offense for the improper handling or disclosure of classified information that may or may not be NDI;

4) better define NDI than simply being any information that "relates" to the "nation's military activities, intelligence, or foreign policy"; this is facially too broad, especially as to foreign policy; a better definition would include words like "describes" or some narrower concept than "relates" and the phrase "foreign policy" is too broad and should either be omitted or carefully limited;

5) include the requirement that NDI has to be "closely held"; right now, some officials state that it does not matter if a piece of information is completely out in the public as long as a new government official's disclosure of it "can confirm" its existence; there are occasions when information is so available and pervasive that it can no longer be said to be "closely held";

6) define the *mens rea* (criminal intent) required for each offense in terms that are clear so people can conform their conduct and judges and juries can apply the law evenly and consistently when it is violated; here a good starting point is to require

the government to prove beyond a reasonable doubt that a defendant acted with the intent to injure the United States and, when the First Amendment is implicated, that there was an apparent "clear and present danger" for injury to occur; disclosures without that intent can still be punished, but less severely; and

7) make clear how the law covers tangible as well as non-tangible information in a manner that protects First Amendment activity and whether and how, in the context of "leaks," it should ever be applied to those who are not government officials, especially to those engaged in free speech, free press or petitioning the government for redress (in other words the First Amendment).

J. Conclusion

As is always the case, a current, big story can be the catalyst for congressional oversight. This is good. A meaningful debate about the Espionage Act and changes to the law are long overdue. However, a current scandal or crisis is not the time to act too quickly. There is often an urge to address the clamor of the crisis to show that Washington is listening and doing something and taking a problem seriously. This can lead to ill-conceived laws that have unintended consequences that infringe on rights and cause decades of needless litigation. Indeed, whatever WikiLeaks and Mr. Assange have done, they have done. A new law would not apply to these past acts under the prohibition against *ex post facto* laws. So, the current issues are a very good opportunity to do the careful review and sifting of the national security values we have to protect and balance them against the rights we cherish. There is no doubt that an effective law can be crafted to address espionage, improper disclosure of national defense information, and improper dissemination of classified information, but this will require the kind of painstaking consideration that these hearings have begun, reference to the current case law,

the input of the national security community and the scholarly community that will take a little time.

Courts that have grappled with the Espionage Act have been constrained by having to apply its existing structure and language. Obviously, Congress is not so limited. The point is that there is a real opportunity, that these and similar hearings recognize, to create a tough law, a clear law, and a law that also can respect the values we place on a free speech and open government.

You, your colleagues and your staff are to be commended for taking on this project at a time when it would be just as easy to let the current flawed statute exist for another 100 years or to let someone else do this hard analysis. I hope that these observations and suggestions are helpful in some way, and I would be glad to provide more information or any additional assistance I can to this effort.

# # #