McDermott
Will & Emery

Boston Brussels Chicago Düsseldorf London Los Angeles Miami Munich
New York Orange County Rome San Diego Silicon Valley Washington, D.C.
Strategic alliance with MWE China Law Offices (Shanghai)

May 7, 2009

Abbe David Lowell
Attorney at Law
adlowell@mwe.com
202.756.8001

VIA EMAIL AND FIRST CLASS MAIL

Honorable Benjamin L. Cardin
Chairman
Subcommittee on Terrorism and Homeland Security
Senate Committee on the Judiciary
SH-815 Hart Senate Office Building
Washington, D.C. 20510-6288

Re: Hearings On The Espionage Act of 1917

Dear Chairman Cardin:

I appreciate your invitation to address some of the issues raised by The Espionage Act of 1917 ("the Act") for which you are holding hearings. My involvement with the law and its related statutes (e.g., the Classified Information Protection Act) 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 so-called American-Israeli Public Affairs Committee [AIPAC] case and am working on an active Espionage Act investigation now).

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 make equally serious 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, and mishandling of classified information – should be set our 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, however, is that its antiquated structure still lumps or can lump these three separate forms of violation in the same sections of the statute. That neither serves justice well when it seeks to address the most egregious conduct (e.g. a government official who, for money or misplaced loyalty, provide NDI to an adversary) nor does it promote 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).

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 addressing, but it is an important consideration when a law criminalizes disclosure of such material. As many others have indicated, "when everything is classified, nothing really is classified." 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. 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. In any event, this is an issue for another time.

What is primarily missing in the Act right now is clarity. The statute has been attacked often as vague and overbroad (we did that ourselves in the AIPAC 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.

To save the law, courts have bent and twisted the Act's language to engraft various evidentiary requirements to confirm it to both the First Amendment and Due Process Clauses. Still it is a morass:

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

- How does one even measure "potentially damaging" (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 scienter requirement mean that a person has to purposely intend to disclosure what he or she knows is being kept confidential or do so also with the intent to injure our country or assist another? Especially in the First Amendment context, should not there be the higher requirement?

- 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 or have done themselves versus when they are violating the rules?

- 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.

The AIPAC case itself 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 for years. 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 (Steven Rosen and Keith Weissman) investigated, they were charged with violating The Espionage Act of 1917. 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 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 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.

That the same section or sections of the Act can be used to prosecute this conduct along side with former FBI agent turned Russian spy Robert Hannsen shows 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, in the hands of ill-intended investigators and prosecutors, 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.

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. Even so, the Act was criticized when it was passed and almost every decade later for issues similar to those I raise in this letter. A newly formulated statute should:

1) carefully define espionage to prohibit the seeking or receipt of national defense information 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 a way that does 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 country;

3) define and properly punish a separate offense for the improper handing 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" has to be carefully limited;

5) one requirement for information to be NDI is that it 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* 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;

7) clearly distinguish between disclosure with the intent to injure the U.S. or assist an adversary and disclosure that do not have that purpose; and

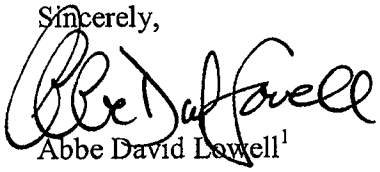
8) make clear how the law covers tangible as well as non-tangible information in a manner that protects First Amendment activity and whether and how, in the

context of "leak," it should ever be applied to those who are not government officials.

There is a great deal of case law that can instruct this oversight exercise. However, courts have been constrained to use the existing structure and language of the statute in applying it. Obviously, Congress is not so limited. The point is that there is a real opportunity that your 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 someone else do it or wait for another time. I hope that these observations and suggestions are helpful in any way, and I would be very glad to provide more information or any additional assistance I can to this effort.

Sincerely,



Abbe David Lowell[1]

[1] This letter reflects my own views and not the firm's or any client's. The stationery is being used only as a form of identification.