

ESPIONAGE ACT AND THE LEGAL AND CONSTITUTIONAL ISSUES RAISED BY WIKILEAKS

HEARING BEFORE THE COMMITTEE ON THE JUDICIARY HOUSE OF REPRESENTATIVES ONE HUNDRED ELEVENTH CONGRESS SECOND SESSION

DECEMBER 16, 2010

Serial No. 111-160

Printed for the use of the Committee on the Judiciary



Available via the World Wide Web: <http://judiciary.house.gov>

U.S. GOVERNMENT PRINTING OFFICE

63-081 PDF

WASHINGTON : 2011

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512-1800; DC area (202) 512-1800
Fax: (202) 512-2104 Mail: Stop IDCC, Washington, DC 20402-0001

COMMITTEE ON THE JUDICIARY

JOHN CONYERS, JR., Michigan, *Chairman*

HOWARD L. BERMAN, California	LAMAR SMITH, Texas
RICK BOUCHER, Virginia	F. JAMES SENSENBRENNER, JR., Wisconsin
JERROLD NADLER, New York	HOWARD COBLE, North Carolina
ROBERT C. "BOBBY" SCOTT, Virginia	ELTON GALLEGLY, California
MELVIN L. WATT, North Carolina	BOB GOODLATTE, Virginia
ZOE LOFGREN, California	DANIEL E. LUNGREN, California
SHEILA JACKSON LEE, Texas	DARRELL E. ISSA, California
MAXINE WATERS, California	J. RANDY FORBES, Virginia
WILLIAM D. DELAHUNT, Massachusetts	STEVE KING, Iowa
STEVE COHEN, Tennessee	TRENT FRANKS, Arizona
HENRY C. "HANK" JOHNSON, JR., Georgia	LOUIE GOHMERT, Texas
PEDRO PIERLUISI, Puerto Rico	JIM JORDAN, Ohio
MIKE QUIGLEY, Illinois	TED POE, Texas
JUDY CHU, California	JASON CHAFFETZ, Utah
TED DEUTCH, Florida	TOM ROONEY, Florida
LUIS V. GUTIERREZ, Illinois	GREGG HARPER, Mississippi
TAMMY BALDWIN, Wisconsin	
CHARLES A. GONZALEZ, Texas	
ANTHONY D. WEINER, New York	
ADAM B. SCHIFF, California	
LINDA T. SANCHEZ, California	
DANIEL MAFFEI, New York	
JARED POLIS, Colorado	

PERRY APELBAUM, *Majority Staff Director and Chief Counsel*
SEAN MCLAUGHLIN, *Minority Chief of Staff and General Counsel*

CONTENTS

DECEMBER 16, 2010

	Page
OPENING STATEMENTS	
The Honorable John Conyers, Jr., a Representative in Congress from the State of Michigan, and Chairman, Committee on the Judiciary	1
The Honorable Louie Gohmert, a Representative in Congress from the State of Texas, and Member, Committee on the Judiciary	3
The Honorable William D. Delahunt, a Representative in Congress from the State of Massachusetts, and Member, Committee on the Judiciary	4
The Honorable Howard Coble, a Representative in Congress from the State of North Carolina, and Member, Committee on the Judiciary	5
The Honorable Charles A. Gonzalez, a Representative in Congress from the State of Texas, and Member, Committee on the Judiciary	5
The Honorable Ted Poe, a Representative in Congress from the State of Texas, and Member, Committee on the Judiciary	5
WITNESSES	
Mr. Geoffrey R. Stone, Professor and former Dean, University of Chicago Law School	
Oral Testimony	6
Prepared Statement	9
Mr. Abbe David Lowell, Partner, McDermott Will & Emery, LLP	
Oral Testimony	22
Prepared Statement	25
Mr. Kenneth L. Wainstein, Partner, O'Melveny & Myers, LLP	
Oral Testimony	39
Prepared Statement	41
Mr. Gabriel Schoenfeld, Ph.D., Senior Fellow, Hudson Institute	
Oral Testimony	48
Prepared Statement	50
Mr. Stephen I. Vladeck, Professor of Law, American University	
Oral Testimony	66
Prepared Statement	69
Mr. Thomas S. Blanton, Director, National Security Archive, George Washington University	
Oral Testimony	74
Prepared Statement	77
Mr. Ralph Nader, Legal Advocate and Author	
Oral Testimony	87

ESPIONAGE ACT AND THE LEGAL AND CONSTITUTIONAL ISSUES RAISED BY WIKILEAKS

THURSDAY, DECEMBER 16, 2010

HOUSE OF REPRESENTATIVES,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The Committee met, pursuant to notice, at 10:05 a.m., in room 2141, Rayburn House Office Building, the Honorable John Conyers, Jr. (Chairman of the Committee) presiding.

Present: Representatives Conyers, Scott, Jackson Lee, Delahunt, Johnson, Quigley, Gutierrez, Schiff, Sensenbrenner, Coble, Gallegly, Goodlatte, King, Frank, Gohmert, Poe, and Harper.

Staff Present: (Majority) Perry Apelbaum, Staff Director and Chief Counsel; Elliot Minberg, Counsel; Sam Sokol, Counsel; Joe Graupensberger, Counsel; Nafees Syed, Staff Assistant; (Minority) Caroline Lynch, Counsel; Kimani Little, Counsel; and Kelsey Whitlock, Clerk.

Mr. CONYERS. Good morning. The hearing on the Espionage case and the legal and constitutional issues raised by WikiLeaks before the Committee on Judiciary is now about to take place. We welcome everyone here to the hearing. In the *Texas v. Johnson* case in 1989, the Supreme Court set forth one of the fundamental principles of our democracy. That is, that if there is a bedrock principle underlying the First Amendment, it is that the government may not prohibit the expression of an idea simply because society finds the idea itself offensive or disagreeable.

That was Justice William Brennan. Today the Committee will consider the WikiLeaks matter. The case is complicated, obviously. It involves possible questions of national security, and no doubt important subjects of international relations, and war and peace. But fundamentally, the Brennan observation should be instructive.

As an initial matter, there is no doubt that WikiLeaks is in an unpopular position right now. Many feel their publication was offensive. But unpopularity is not a crime, and publishing offensive information isn't either. And the repeated calls from Members of Congress, the government, journalists, and other experts crying out for criminal prosecutions or other extreme measures cause me some consternation.

Indeed, when everyone in this town is joined together calling for someone's head, it is a pretty sure sign that we might want to slow down and take a closer look. And that is why it was so encouraging

to hear the former Office of Legal Counsel, Jack Goldsmith, who served under George W. Bush caution us only last week. And he said, I find myself agreeing with those who think Assange is being unduly vilified. I certainly do not support or like his disclosure of secrets that harm U.S. national security or foreign policy interests. But as all the handwringing over the 1917 Espionage Act shows, it is not obvious what law he has violated.

Our country was founded on the belief that speech is sacrosanct, and that the answer to bad speech is not censorship or prosecution, but more speech. And so whatever one thinks about this controversy, it is clear that prosecuting WikiLeaks would raise the most fundamental questions about freedom of speech about who is a journalist and about what the public can know about the actions of their own government.

Indeed, while there's agreement that sometimes secrecy is necessary, the real problem today is not too little secrecy, but too much secrecy. Recall the Pentagon papers case, Justice Potter Stewart put it, when everything is classified, nothing is classified. Rampant overclassification in the U.S. system means that thousands of soldiers, analysts and intelligence officers need access to huge volumes of purportedly classified material. And that necessary access in turn makes it impossible to effectively protect truly vital secrets.

One of our panelists here today put it perfectly in a recent appearance. He explained, our problem with our security system, and why Bradley Manning can get his hands on all these cables, is we got low fences around a vast prairie because the government classifies just about everything. What we really need are high fences around a small graveyard of what is really sensitive. Furthermore, we are too quick to accept government claims that risk the national security and far too quick to forget the enormous value of some national security leaks. As to the harm caused by these releases most will agree with the Defense Secretary, Bob Gates, his assessment.

Now, I have heard the impact of these releases on our foreign policy described as a meltdown, as a game changer, and so on. I think those descriptions are fairly significantly overwrought. And Mr. Gates continues, is this embarrassing? Yes. Is it awkward? Yes. Consequences for U.S. policy? I think fairly modest.

So the harm here, according to our Republican Defense Secretary, is fairly modest. Among the other side of the ledger, there is no need to go all the way back to the Pentagon papers to find examples of national security leaks that were critical to stopping government abuses and preserving a healthy democracy. They happen all the time.

In 2005, The New York Times published critical information about widespread domestic surveillance. Ultimately, we learned of a governmental crisis that included threats of mass resignations at the Justice Department and outrageous efforts to coerce a sick attorney general into approving illegal spying over the objections of his deputy and legal counsel's office. If not for this leak, we would have never learned what a civil libertarian John Ashcroft is.

In 2004, the leak of a secret office of legal counsel interrogation memos led to broader revelations of the CIA's brutal enhanced interrogation programs at Black sites. These memos had not been

previously revealed to the Judiciary Committee or to many in Congress. Some feel this harmed national security. But to many Americans, the harm was a secret program of waterboarding and other abuses that might never have been ended but for the leak.

And so we want to, as the one Committee in the Congress that I have a great and high regard for, take a closer look at the issues and consider what, if any, changes in the law might be necessary. And I want to welcome this very distinguished panel. I have read late into the night, and I was awake most of the time when I was reading this, some really great testimony. And I am so glad that you are all here with us. I would like now to recognize my friend and Ranking Member, Judge Louie Gohmert.

Mr. GOHMERT. Thank you, Chairman. And I do appreciate the witnesses here. Before I begin my actual statement, let me just say I appreciate, and am also intrigued by your metaphorical use of the need for high fences around a small graveyard. But I am curious, are you saying this Administration is located in a small graveyard? Is that the point?

Mr. CONYERS. See me after the hearing, please, Judge Gohmert.

Mr. GOHMERT. Thank you, Chairman. And I appreciate the Ranking Member Smith asking me to stand in. But the release last month by WikiLeaks of over 250,000 classified and diplomatic U.S. documents threatens our national security, our relations with foreign governments, and continued candor from embassy officials and foreign sources. Many have applauded the Web site and its founder, Julian Assange, as a hero advocating the continued release of classified and sensitive government documents. But to do so is both naive and dangerous. Web sites such as WikiLeaks and the news publications that reprint these materials claim to promote increased government transparency.

But the real motivation is self-promotion and increased circulation to a large extent. They claim to be in pursuit of uncovering government wrongdoing but dismiss any criticism that their actions may be wrong or damaging to the country. As long as there have been governments, there have been information protected by those governments. There have clearly been documents classified that should not have been classified. While there is legitimate dispute over the extent to which information is protected and classified, it is simply unrealistic to think that the protection of information serves no legitimate purpose.

Much attention has been given to this most recent WikiLeaks release. Many dismiss that any negative repercussions resulted from the leak arguing that the documents, while embarrassing to the U.S., did no real harm to the country. But what about previous leaks by this Web site? On July 25, 2010, WikiLeaks released confidential military field reports on the war in Afghanistan. This site released Iraq war-related documents on October 23, 2010. Both of these leaks reveal sensitive military information that endanger military troops and may have bolstered our enemy's campaigns against us.

Last month's WikiLeaks release has thrust in the spotlight an old, some would even say, arcane statute, the Espionage Act of 1917. It has also resurrected an age-old debate on First Amendment protections afforded to media publications.

But today we are confronted with a new kind of media, the Internet blog. What are the boundaries of free speech, how do we balance this freedom with the Government's need to protect some information. The drafters of the 1917 Act could not have foreseen that nearly 100 years later, sensitive information could have been transmitted to a global audience instantaneously. America's counterterrorism efforts must respond to new and emerging threats such as home-grown terrorism. Our criminal laws must also keep pace with advancing technologies that enable widespread dissemination of protected information. This time the leak involved primarily diplomatic cables, but previous leaks disclosed even more sensitive information.

And the next leak could be even more damaging. It could disclose accordance of where military personnel are located overseas or even reveal the next unannounced visit to Iraq or Afghanistan by President Obama. This isn't simply about keeping government secrets secret, it is about the safety of American personnel overseas at all levels from the foot soldier to the commander-in-chief.

With that, Mr. Chairman, I yield back.

Mr. CONYERS. Thank you, Judge Gohmert. This may be the last time that we have an opportunity to recognize our good friend, Bill Delahunt of Massachusetts. He has served the Committee in a very important way, and we yield to him at this time.

Mr. DELAHUNT. Well, thank you, Mr. Chairman. You know, as you are aware, I also serve on the Foreign Affairs Committee. And during that service, I had the opportunity to Chair the Committee on Oversight. And I must say, and this is true of both the Bush and the Obama administrations, it was difficult for me in that capacity, and it was difficult for the Chair of the full Committee, to secure information from the executive. I would submit that this particular hearing should be viewed in a much larger context. Leaks that obviously put people at risk, that put the United States at risk and methods, et cetera, there has to be parameters.

But I think we are at a moment in our history where there is an overwhelming overclassification of material. And I think that we, in our role as Members of the first branch of government, ought to examine very, very carefully that the classification procedures. When you inquire of any executive agency and pose the very simple question, well, why is it classified? It is extremely difficult to get a direct and clear answer. Who does the classification? Is it the Secretary of State or the Attorney General? Who does the classification? During the course of my service, I discovered it was some low-level bureaucrat.

And the process itself is arcane, and there is no accountability, I dare say, in the classification processes that exist within the executive branch. And that is very dangerous, because secrecy is the trademark of totalitarianism. To the contrary, transparency and openness is what democracy is about. So while there is a focus now on the issue of WikiLeaks, I think it provides an opportunity for this Committee, and I think this is a concern that is shared by both Republicans and Democrats, about the classification process itself. There is far too much secrecy and overclassification within the executive branch, and I think it puts American democracy at risk. And with that I yield back.

Mr. CONYERS. Thank you, Bill. I am pleased now to turn to Howard Coble of North Carolina, a senior Member, who will soon be Chair of at least one Subcommittee, maybe two, we don't know yet.

Mr. COBLE. Mr. Chairman, you are more optimistic than I am, but I appreciate that. I have no detailed statement. I want to associate my remarks—yield my remarks regarding the gentleman from Massachusetts. He will indeed be missed on this Committee. This is a crucial issue as known to all of us. And not unlike many crucial issues, and perhaps most crucial issues, it is laced very generously with complications. Good to have the panel with us. And, Mr. Chairman, I yield back.

Mr. CONYERS. Judge, would you care to make an opening comment?

Mr. GONZALEZ. Mr. Chairman, I do not have any opening comments regarding the testimony and such, just looking forward to it. But I do want to just say good-bye to Bill. Obviously, of the Massachusetts delegation, he is the one Member that I can clearly understand despite that accent of theirs. But truly, he has been a good friend, and again, just such a valuable Member to the House, and he will be missed. But I am hoping that, of course, he made the decision because he is moving on to something that is going to be even more rewarding than what he has done here in Congress. Again, thank you very much, Mr. Chairman, for the opportunity. I yield back.

Mr. CONYERS. Thank you, Judge Gonzalez. Judge Ted Poe, I would recognize you at this time, sir.

Mr. POE. Thank you, Mr. Chairman. I ditto what has been said about Bill Delahunt, a wonderful Member of this Committee, hate to see him go, although we disagreed probably on everything.

A couple comments about this situation. I see two issues. One issue is we got to find the original leak and what caused it, who did it and hold them accountable. The other issues that this brings forth is the fact that after 9/11, the big talk was we need to share information with different agencies in the United States Government because we don't know what one agency is doing or knows that should be shared. And so now we have mass sharing and now we seem like we are going to move away from that because of this situation.

I have no sympathy for the alleged thief in this situation. He is no better than a Texas pawnshop dealer that deals in stolen merchandise and sells it to the highest bidder, but he is doing it for political gain. He should be held accountable. But, on the other hand, I am very concerned about our own overclassification of information. The easiest way for a government agency to take information is to say, it is classified, only special folks get to know what is in it. And I have been to a lot of classified briefings. And frankly, I have read a lot of that in the newspaper before that meeting ever took place, and it wasn't classified. Somebody just decides to make it classified and then you have that whole problem of overclassification of documents.

And lastly, the security of our information is important. And we have to—those who allowed this to occur by incompetence, negligence, or whatever, we have to fix that problem. I am very concerned about that because of the fact that, you know, I suppose we

are the greatest and most powerful Nation that ever existed, and we need to ratchet up our security to keep hackers from getting into it, and why did this occur and who allowed it to occur and what went wrong to make this situation now go worldwide?

It is like a bunch of folks at a bank decide to hold a Christmas party down the street and they all take off and leave the vault open. You know, there is a security problem with that kind of thing. And so I would hope that we would fix the security problem, find out what occurred and how it did occur. We ought to think through the idea of overclassification. And then thieves for political reasons or any other reasons, they also need to be held accountable. I yield back.

Mr. CONYERS. Thank you, Judge Poe. We welcome our witnesses, all seven. Ralph Nader, Professor Steve Vladeck, Mr. Gabriel Schoenfeld, Attorney Kenneth Wainstein, Thomas Blanton, Director of the National Security Archive, Attorney Abbe Lowell, well known to this Committee and to previous congresses.

And our first witness, Professor Geoffrey Stone, Professor of Law and Former Dean of the University of Chicago Law School. He has written quite a bit on constitutional law, several books, *The First Amendment*, *Government Power*. One of his books, *Perilous Times*, *Free Speech in War Time*, was just recently praised by Justice Elena Kagan as a masterpiece of constitutional history that promises to redefine the national debate on civil liberties and free speech.

We are honored by you being here, and we ask you to be our first witness. And all the statements of all of our witnesses will be introduced in their entirety into the record. Welcome.

**TESTIMONY OF GEOFFREY R. STONE, PROFESSOR AND
FORMER DEAN, UNIVERSITY OF CHICAGO LAW SCHOOL**

Mr. STONE. Chairman Conyers, Judge Gohmert, Members of the Committee, thank you very much for inviting me and giving me this opportunity to speak with you about these issues. What I would like to do is address the constitutionality of the proposed SHIELD Act, which has been introduced in both Houses of Congress.

The SHIELD Act would amend the Espionage Act of 1917 to make it a crime for any person knowingly and willfully to disseminate in any manner, prejudicial to the safety or interest of the United States, any classified information concerning human intelligence activities of the United States.

Now, although this act might be constitutional as applied to government employees who unlawfully leak such material to persons who are unauthorized to receive it, it is plainly unconstitutional as applied to other individuals or organizations who might publish or otherwise disseminate the information after it has been leaked. With respect to such other speakers, the Act violates the First Amendment unless, at the very least, it is expressly limited to situations in which the dissemination of the specific information at issue poses a clear and imminent danger of grave harm to the Nation.

The clear and present danger standard in varying forms has been a central element of our First Amendment jurisprudence ever

since Justice Oliver Wendell Holmes first enunciated it in his 1919 opinion in *Schenck v. the United States*. In the 90 years since Schenck, the precise meaning of clear and present danger has evolved, but the principle that animates it was stated eloquently by Justice Louis Brandeis in his brilliant 1927 concurring opinion in *Whitney v. California*. “Those who won our independence,” wrote Brandeis, “did not exalt order at the cost of liberty. They understood that only an emergency can justify repression. Such,” he said, “must be the rule if authority is to be reconciled with freedom. Such is the command of the Constitution. It is therefore always open to challenge a law abridging free speech by showing that there was no emergency justifying it.”

This principle is especially powerful in the context of government efforts to suppress speech concerning the activities of the government itself. As James Madison observed, “a popular government without popular information with the means of acquiring it is but a prologue to a forest or a tragedy or perhaps both.” As Madison warned, if citizens do not know what their own government is doing, then they are hardly in a position to question its judgments or to hold their elected representatives accountable.

Government secrecy, although surely necessary at times, can also pose a direct threat to the very idea of self-governance. Nonetheless, the First Amendment does not compel government transparency. It leaves the government extraordinary autonomy to protect its own secrets. It does not accord anyone the right to have the government disclose information about its actions or policies, and it cedes to the government considerable authority to restrict the speech of its own employees.

What it does not do, however, is to leave the government free to suppress the free speech of others when it has failed itself to keep its own secrets. At that point, the First Amendment kicks in with full force. And as Brandeis explained, only an emergency can then justify suppression. We might think of this like the attorney/client privilege. The client is free to keep matters secret by disclosing them to no one. He is also free to disclose certain matters to his attorney, who is under a legal obligation to respect the confidentiality of the client’s disclosures.

In this sense, the attorney is sort of like the government employee. If the attorney violates the privilege by revealing the client’s confidences, say, to a reporter, then the attorney can be punished for doing so, but the newspaper cannot constitutionally be punished for disseminating the information.

Now, some may wonder whether it makes sense to give the government so little authority to punish the dissemination of unlawfully leaked information, but there are sound reasons for insisting on a showing of clear and present danger before the government can punish speech in this context.

First, the mere fact that the dissemination of such information might, in the words of the proposed Act, in any matter, “prejudice the interest of the United States” does not mean that the harm outweighs the benefit of publication, as Chairman Conyers noted. In many circumstances, such information may indeed be extremely valuable to public understanding.

Second, a case-by-case balancing of harm against benefit would be unwieldy, unpredictable and impracticable. Clear rules are essential in the realm of free speech. Indeed, that is one reason why we grant the government so much authority to restrict the speech of its own employees, rather than insisting that in every case the government must demonstrate that the harm outweighs the benefit.

Third, as we have learned from our own history, there are great pressures that lead both government officials and even the public to overstate the potential harm of publication in times of national anxiety. A strict clear and present danger standard serves as a barrier to protect us against that danger.

And finally, a central principle of the First Amendment is that the suppression of public speech must be the government's last rather than its first resort in addressing a potential problem. If there are other means by which the government can prevent or reduce the danger, it must exhaust those other means before it can even entertain the prospect of suppressing the freedom of speech.

In the secrecy situation, the most obvious and the correct way for government to prevent the danger is by ensuring that information that must be kept secret is kept secret, and is not leaked in the first place. Indeed, the Supreme Court made this very point less than a decade ago in a case known as *Bartnicki v. Vopper*, in which the court held that when an individual receives information from a source who has obtained it unlawfully, that individual may not be punished for publicly disseminating the information "absent a need of the highest order."

The Court explained that "if the sanctions that presently attach to the underlying criminal act do not provide sufficient deterrence, then perhaps those sanctions should be made more severe." But it would be, the Court said, "quite remarkable to hold that an individual can constitutionally be punished merely for disseminating information because the government itself failed to deter conduct by a nonlaw abiding party."

This may seem a disorderly situation, but the court has, in fact, come up with a good solution. If we grant the government too much power to punish those who disseminate information, then we risk too great a sacrifice of public deliberation. If we grant the government too little power to control confidentiality at the source, then we risk too great a sacrifice of secrecy. The solution is to reconcile the irreconcilable values of secrecy, on the one hand, and accountability, on the other, by guaranteeing both a strong authority of the government to prohibit leaks, and an expansive right of others to disseminate information to the public.

The bottom line then is this: The proposed SHIELD Act is unconstitutional. At the very least, it must limit its prohibition to those circumstances in which the individuals who publicly disseminated classified information knew that the dissemination would create a clear and imminent danger of grave harm to our Nation or our people. Thank you.

Mr. CONYERS. Thank you very much, Professor.
[The prepared statement of Mr. Stone follows:]

PREPARED STATEMENT OF GEOFFREY R. STONE

Statement of Geoffrey R. Stone
Edward H. Levi Distinguished Service Professor of Law
The University of Chicago

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

Committee on the Judiciary
United States House of Representatives

December 16, 2010

The proposed SHIELD Act¹ would amend the Espionage Act of 1917² to make it a crime for any person knowingly and willfully to disseminate, in any manner prejudicial to the safety or interest of the United States, “any classified information . . . concerning the human intelligence activities of the United States or . . . concerning the identity of a classified source or informant” working with the intelligence community of the United States.

Although the Act might be constitutional as applied to a government employee who “leaks” such classified material, it is plainly unconstitutional as applied to other individuals who might publish or otherwise disseminate such information. With respect to such other individuals, the Act violates the First Amendment unless, at the very least, it is expressly limited to situations in which the individual knows that the dissemination of the classified material poses *a clear and present danger of grave harm to the nation*.

The clear and present danger standard, in varying forms, has been a central element of our First Amendment jurisprudence ever since Justice Oliver Wendell Holmes first enunciated it in his 1919 opinion in *Schenck v. United States*.³ In the 90 years since *Schenck*, the precise meaning of “clear and present danger” has shifted,⁴ but the principle that animates the standard was stated eloquently by Justice Louis D. Brandeis in his brilliant 1927 concurring opinion in *Whitney v. California*:⁵

Those who won our independence by revolution were not cowards. . . . They did not exalt order at the cost of liberty. . . . Only an emergency can justify repression. Such must be the rule if authority is to be reconciled with freedom. Such . . . is the command of the Constitution. It is, therefore, always open to Americans to challenge a law abridging free speech . . . by showing that there was no emergency justifying it.

With that observation in mind, I will examine two central questions: (1) Does the clear and present danger standard apply to unlawful leaks of classified information by public employees? (2) Does the clear and present danger standard apply to the dissemination of classified information derived from those unlawful leaks? These are fundamental First Amendment questions. Before turning to them, though, a bit of historical context is necessary.

¹ H.R. 2695, 111th Cong., 2d Sess. (2010).

² 18 U.S.C. 798

³ *Schenck v. United States*, 249 U.S. 47, 52 (1919).

⁴ See Frank Strong, *Fifty Years of “Clear and Present Danger”: From Schenck to Brandenburg – and Beyond*, 1969 Sup. Ct. Rev. 41. Compare *Schenck v. United States*, 249 U.S. 47, 52 (1919); *Dennis v. United States*, 341 U.S. 494 (1951); *Brandenburg v. Ohio*, 395 U.S. 444 (1969); and *New York Times v. United States*, 403 U.S. 713 (1971). See generally Geoffrey R. Stone, *Perilous Times: Free Speech in Wartime from 1790 to the War on Terrorism* (W. W. Norton 2004).

⁵ 274 U.S. 357, 377 (1927) (Brandeis, J., concurring).

I. National Security and Free Speech

A wartime environment inevitably intensifies the tension between individual liberty and national security. But there are wise and unwise ways to strike the appropriate balance. Throughout American history, our government has excessively restricted public discourse in the name of national security. In 1798, for example, on the eve of a threatened conflict with France, Congress enacted the Sedition Act of 1798, which effectively made it a crime for any person to criticize the president, the Congress or the government itself.⁶ During the Civil War, the government shut down “disloyal” newspapers and imprisoned critics of the president’s policies.⁷ During World War I, the government enacted the Espionage Act of 1917 and the Sedition Act of 1918, which made it unlawful for any person to criticize the war, the draft, the government, the president, the flag, the military, or the cause of the United States, with the consequence that free and open debate was almost completely stifled.⁸ And during the Cold War, as Americans were whipped up to frenzy of fear of the “Red Menace,” loyalty programs, political infiltration, blacklisting, legislative investigations, and criminal prosecutions of supposed Communist “subversives” and sympathizers swept the nation.⁹

Over time, we have come to understand that these episodes from our past were grievous errors in judgment in which we allowed fear and anxiety to override our good judgment and our essential commitment to individual liberty and democratic self-governance. Over time, we have come to understand that, in order to maintain a robust system of democratic self-governance, our government cannot constitutionally be empowered to punish speakers, even in the name of “national security” without a *compelling* justification.¹⁰ And this is especially true in the realm of government secrets, for as James Madison observed, “A popular Government, without popular information, or the means of acquiring it, is but a Prologue to a Farce or a Tragedy; or perhaps both.”¹¹ As Madison warned, if citizens do not know what their own government is doing, then they are hardly in a position to question its judgments or to hold their elected representatives accountable. Government secrecy, although sometimes surely necessary, can also pose a direct threat to the very idea of self-governance.

⁶ See Geoffrey R. Stone, *War and Liberty: An American Dilemma* 1-21 (W. W. Norton 2007).

⁷ See *id.*, at 22-40.

⁸ See *id.*, at 41-63.

⁹ See *id.*, at 85-106.

¹⁰ See Stone, *Perilous Times* at 550-558 (cited in note 4).

¹¹ James Madison, *The Writings of James Madison* (1822), Gaillard Hunt, ed., G. P. Putnam’s Sons (1910).

II. The Dilemma

Here, then, is the dilemma: The government often has exclusive possession of information about its policies, programs, processes, and activities that would be of great value to informed public debate. But government officials often insist that such information must be kept secret, even from those to whom they are accountable – the American people. How should we resolve this dilemma? The issue is complex, and has many dimensions.

The reasons why government officials want secrecy, for example, are many and varied. They range from the truly compelling to the patently illegitimate. Sometimes, government officials may want secrecy because they fear that the disclosure of certain information might seriously undermine the nation's security (for example, by revealing detailed battle plans on the eve of battle). Sometimes, they may want secrecy because they simply do not want to deal with public criticism of their decisions, or because they do not want the public, the Congress, or the courts to be in a position to override their decisions, which they believe to be sound. Sometimes, they may want secrecy because disclosure will expose their own incompetence or foolishness or wrongdoing. Some of these reasons for secrecy are obviously much more worthy of respect than others. Part of the problem is that government officials who want secrecy for questionable reasons are often tempted to "justify" their actions by putting forth seemingly compelling, but in reality exaggerated or even disingenuous, justifications.

Adding to the complexity, the contribution of any particular disclosure to informed public discourse may vary widely depending upon the nature of the information and the surrounding circumstances. The disclosure of some classified information may be extremely valuable to public debate (for example, the revelation of possibly unwise or even unlawful or unconstitutional government programs, such as the secret use of coercive interrogation or the secret authorization of widespread electronic surveillance). The disclosure of other confidential information, however, may be of little or no legitimate value to public debate (for example, the publication of the specific identities of covert American agents in Iran for no reason other than exposure).

The most vexing problem arises when the public disclosure of secret information is both harmful to the national security *and* valuable to self-governance. Suppose, for example, the government undertakes a study of the effectiveness of security measures at the nation's nuclear power plants. The study concludes that several nuclear power plants are especially vulnerable to terrorist attack. Should this study be kept secret or should it be disclosed to the public? On the one hand, publishing the report will reveal our vulnerabilities to terrorists. On the other hand, publishing the report would alert the public to the situation, enable citizens to press government officials to remedy the problems, and empower the public to hold accountable those public officials who failed to keep them safe. The public disclosure of such information could both harm and benefit the nation. Should the study be made public?

In theory, this question can be framed quite simply: Do the benefits of disclosure outweigh its costs? That is, does the value of the disclosure to informed public deliberation outweigh its danger to the national security? Alas, as a practical matter this simple framing of the issue is not terribly helpful. It is exceedingly difficult to measure in any objective, consistent, predictable, or coherent manner either the “value” of the disclosure to public discourse or its “danger” to national security. And it is even more difficult to balance such incommensurable values against one another.

Moreover, even if we were to agree that this is the right question, we would still have to determine who should decide whether the benefits outweigh the costs of disclosure. Should this be decided by public officials whose responsibility it is to protect the national security? By public officials who might have an incentive to cover up their own mistakes? By low-level public officials who believe their superiors are keeping information secret for inadequate or illegitimate reasons – that is, by “leakers”? By reporters, editors, bloggers, and others who have gained access to the information? By judges and jurors, in the course of criminal prosecutions of leakers, journalists, and publishers?

In this statement, I will focus on two questions: First, in what circumstances can the government constitutionally punish a public employee for *disclosing* classified information to a journalist for the purpose of publication? That is, in what circumstances may the government punish “leakers”? Second, in what circumstances can the government constitutionally punish the *publication or public dissemination* of classified information? Should it matter whether the publisher or disseminator obtained the information through an illegal leak?

III. The Rights of Public Employees

The first question concerns the First Amendment rights of public employees. To understand those rights, we must establish a baseline. Let us begin, then, with the rights of individuals who are *not* government employees. That is, in what circumstances may ordinary people, who are *not* public employees, be held legally accountable for revealing information to another for the purpose of publication? Answering that question will enable us to establish a baseline definition of First Amendment rights. We can then inquire whether the First Amendment rights of government employees are any different.

In general, an ordinary individual (that is, an individual who is not a government employee) has a broad First Amendment right to reveal information to journalists or others for the purpose of publication. There are a few limitations, however.

First, the Supreme Court has long recognized that there are certain “limited classes of speech,” such as false statements of fact, obscenity, and threats, that “are no essential part of any exposition of ideas” and are therefore of only “low” First Amendment

value.¹² Such speech may be restricted without satisfying the usual demands of the First Amendment. For example, if X makes a knowingly false and defamatory statement about Y to a journalist, with the understanding that the journalist will publish the information, X might be liable to Y for the tort of defamation.¹³

Second, private individuals sometimes voluntarily contract with other private individuals to limit their speech. Violation of such a private agreement may be actionable as a breach of contract. For example, if X takes a job as a salesman and agrees as a condition of employment not to disclose his employer's customer lists to competitors, he might be liable for breach of contract if he reveals the lists to a reporter for a trade journal, with the expectation that the journal will publish the list. In such circumstances, the individual has voluntarily agreed to limit what otherwise would be a First Amendment right. Such privately negotiated waivers of constitutional rights are generally enforceable.¹⁴

Third, there may be situations, however rare, in which an individual discloses previously non-public information to a journalist in circumstances in which publication of the information would be so dangerous to society that the individual might be punishable for disclosing the information to the journalist for purposes of further dissemination. For example, suppose a privately-employed scientist discovers how to manufacture anthrax bacteria at home. The harm caused by the public dissemination of that information might be so likely, imminent, and grave that the scientist could be punished for facilitating its publication.¹⁵

These examples illustrate the few circumstances in which an individual might be held legally responsible for disclosing information to another for the purpose of public dissemination. In general, however, the First Amendment guarantees individuals *very* broad freedom to share information with others for the purpose of publication.

To what extent is a *government employee* in a similar position? When we ask about the First Amendment rights of public employees, we must focus on the *second* of the three situations examined above. That is, it is the waiver of rights issue that poses the critical question. Although the first and third situations can arise in the public employee context, it is the waiver issue that is at the core of the matter.

At its most bold, the government's position is simple: Just like a private individual, it should be able to enter into contracts with people in which they voluntarily agree to waive their constitutional rights. As long as the waiver is voluntary, that should end the matter. That is not the law. The Supreme Court has long recognized that, unlike private entities, the government *cannot* constitutionally insist that individuals surrender their constitutional rights as a condition of public employment or receipt of other

¹² *Chaplinsky v. New Hampshire*, 315 U.S. 568, 571-72 (1942).

¹³ See *Gertz v. Robert Welch, Inc.*, 418 U.S. 323 (1974).

¹⁴ See *Cohen v. Cowles Media Co.*, 501 U.S. 663 (1991).

¹⁵ See *United States v. The Progressive*, 467 F. Supp. 990 (W.D. Wis. 1979).

government benefits. It would be unconstitutional, for example, for the government to require individuals to agree as a condition of government employment that they will never criticize the President, never practice the Muslim faith, never have an abortion, or never assert their constitutional right to be free from unreasonable searches and seizures.¹⁶

It would be no answer for the government to point out that the individuals had *voluntarily* agreed not to criticize the President, practice their faith, have an abortion, or assert their Fourth Amendment rights, for even if individuals consent to surrender their constitutional rights in order to obtain a government job, the government cannot constitutionally condition employment on the waiver of those rights. As the Supreme Court has long held, “unconstitutional conditions” on public employment violate the Constitution. The government cannot legitimately use its leverage over jobs, welfare benefits, driver’s licenses, tax deductions, zoning waivers, and the like to extract waivers of individual freedoms.¹⁷

This does not mean, however, that the government can *never* require individuals to waive their constitutional rights as a condition of public employment. There are at least two circumstances, relevant here, in which the government may restrict the First Amendment rights of its employees. First, as the Supreme Court recognized in its 1968 decision in *Pickering v. Board of Education*, the government “has interests as an employer in regulating the speech of its employees that differ significantly from those it possesses in connection with regulation of the speech of the citizenry in general.”¹⁸ The problem, the Court said, is to arrive at a sensible balance between the interests of the public employee, as a citizen, in commenting upon matters of public concern, and the interest of the government, as an employer, in promoting the efficiency of its activities.

The Hatch Act, for instance, prohibits public employees from taking an active part in political campaigns. The goal is to insulate government employees from undue political pressure and improper influence. To enable public employees to perform their jobs properly, the government may require them to waive what would otherwise be the First Amendment right to participate in partisan political activities.¹⁹ Similarly, a government employee’s disclosure of confidential information to a journalist might jeopardize the government’s ability to function effectively. For example, if an IRS employee gives a reporter X’s confidential tax records, this might seriously impair the

¹⁶ See *Perry v. Sinderman*, 408 U.S. 593, 597 (1972) (“even though a person has no ‘right’ to a valuable government benefit and even though the government may deny him the benefit for any number of reasons,” it may not do so “on a basis that infringes his constitutionally protected interests – especially his interest in freedom of speech”).

¹⁷ See Cass R. Sunstein, *Government Control of Information*, 74 Cal. L. Rev. 889, 915 (1986).

¹⁸ 391 U.S. 563, 568 (1968).

¹⁹ See *U.S. Civil Service Commission v. National Association of Letter Carriers*, 413 U.S. 548 (1973); *United States Workers v. Mitchell*, 330 U.S. 75 (1947).

public's confidence in the tax system and thus undermine the government's capacity to function efficiently.

A second reason why the government may sometimes restrict what otherwise would be the First Amendment rights of public employees is that the employee learns the information *only* by virtue of his government employment. Arguably, it is one thing for the government to prohibit its employees from speaking in ways other citizens can speak, but something else entirely for it to prohibit them from speaking in ways other citizens *cannot* speak. If a government employee gains access to confidential information only *because* of his public employment, then prohibiting him from disclosing that information to anyone outside the government might be said not to substantially restrict his First Amendment rights, because he had no right to *know* the information in the first place.²⁰

There is little clear law on this question. In its 1980 decision in *Snepp v. United States*,²¹ however, the Supreme Court held that a former employee of the CIA could constitutionally be held to his agreement not to publish "any information or material relating to the CIA" without prior approval. The Court did not suggest that *every* government employee can be required to abide by such a rule. Rather, it emphasized that a "former intelligence agent's publication of . . . material relating to intelligence activities can be detrimental to vital national interests."²² In light of *Snepp* and *Pickering*, it seems reasonable to assume that a public employee who discloses to a journalist or other disseminator *classified* information, the disclosure of which could appreciably harm the *national security*, has violated his position of trust, and ordinarily may be discharged and/or criminally punished without violating the First Amendment.

Now, it is important to note that this conclusion is specific to public employees. It does not govern those who are *not* public employees. Unlike government employees, who have agreed to abide by constitutionally permissible restrictions of their speech, journalists and others who might disseminate such information have *not* agreed to waive their rights. This distinction between public employees and other individuals is critical in the context of confidential information. Information the government wants to keep secret may be of great value to the public. The public disclosure of an individual's tax return may undermine the public's confidence in the tax system, but it may *also* reveal important information, for example, about a political candidate's finances.

In theory, of course, it would be possible for courts to decide in each instance whether the First Amendment protects an unauthorized disclosure of confidential information by a public employee by decided whether the value of the information to the public outweighs the government's interest in secrecy. But, as I have already noted, such case-by-case judgments would put courts in an exceedingly awkward and difficult

²⁰ See *Seattle Times Co. v. Rhinehart*, 467 U.S. 20 (1984); Robert C. Post, *The Management of Speech: Discretion and Rights*, 1984 Sup. Ct. Rev. 169.

²¹ 444 U.S. 507 (1980).

²² *Id.*, at 511. See also *Haig v. Agee*, 453 U.S. 280 (1981).

position, and would in effect convert the First Amendment into a constitutional Freedom of Information Act. The Supreme Court has eschewed that approach and has instead granted the government considerable deference in deciding whether and when public employees have a constitutional right to disclose confidential government information. In short, the courts have generally held that the government may punish a public employee for the unauthorized disclosure of classified information, as long as the disclosure would be “potentially damaging to the United States.”²³

This is a far cry from requiring the government to prove that the disclosure will create a clear and present danger of grave harm to the nation. The gap between these two standards represents the difference between the rights of public employees and the rights of other individuals. It is what the public employee surrenders as a condition of his employment; it is the effect of *Pickering* balancing; and it is a measure of the deference we grant the government in the management of its “internal” affairs.

There is, of course, a fundamental disadvantage in this approach. Information may be *both* potentially dangerous to national security *and* valuable to public debate. Consider, for example, evaluations of new weapons systems or government policies regulating the permissible conduct of covert agents. One might reasonably argue that this information should be available to the public to enable informed public discussion of such policies. But the approach to public employee speech that I just described ordinarily will empower the government to forbid the disclosure of such information, regardless of its value to public discourse. We accept this approach largely for the sake of simplicity and ease of administration. We should be under no illusions, however, about its impact. This standard gives inordinate weight to secrecy at the expense of accountability and public deliberation.

IV. The Right to Disseminate Information

This, then, brings me to the second question: In what circumstances may the government constitutionally prohibit an individual or organization from *publishing or disseminating* unlawfully leaked classified information? In the entire history of the United States, the government has never prosecuted *anyone* (other than a government employee) for publicly disseminating such information.

Because there has never been such a prosecution, the Supreme Court has never had occasion to rule on such a case. The closest it has come to such a situation was *New York Times v. United States*,²⁴ the Pentagon Papers case, in which the Court held unconstitutional the government’s effort to enjoin the *New York Times* and the *Washington Post* from publishing a purloined copy of a top secret Defense Department study of the Vietnam War. Justice Potter Stewart’s opinion best captures the view of the Court: “We are asked,” he wrote, “to prevent the publication . . . of material that the

²³ *United States v. Morison*, 844 F.2d 1057, 1071-1072 (4th Cir. 1988); *United States v. Rosen*, Case No. 1:05cr225 p. 25 (E.D. Va. 2006) <http://www.fas.org/sgp/jud/rosen080906.pdf>

²⁴ 403 U.S. 713 (1971).

Executive Branch insists should not, in the national interest, be published. I am convinced that the Executive is correct with respect to some of the documents involved. But I cannot say that disclosure of any of them will *surely result in direct, immediate, and irreparable damage to our Nation or its people.*"²⁵

Thus, in the Pentagon Papers case, the Court held that although elected officials have broad authority to keep classified information secret, once that information gets into other hands the government has only very limited authority to prevent its further dissemination. This may seem an awkward, even incoherent, state of affairs. If the government can constitutionally prohibit public employees from disclosing classified information to others, why can't it enjoin the recipients of that material from disseminating it further? But one could just as easily flip the question. If individuals have a First Amendment right to publish classified information unless publication will "surely result in direct, immediate, and irreparable damage to our Nation or its people," why should the government be allowed to prohibit its employees from disclosing that information to others merely because it poses a potential danger to the national security? If we view the issue from the perspective of *either* the public's interest in informed discourse *or* the government's interest in secrecy, it would seem that the same rule logically should apply to both public employees and those who would disseminate the information. The very different standards governing public employees, on the one hand, and other speakers, on the other, thus present a puzzle.

In fact, there are quite sensible reasons for this seemingly awkward state of affairs. Although the government has broad authority to prohibit public employees from leaking classified information, that rule is based not on a careful or definitive balancing of the government's need for secrecy against the public's interest in the information, but on the need for a clear and easily administrable rule for government employees. For the sake of simplicity, the law governing public employees *overprotects* the government's legitimate interest in secrecy relative to the public's legitimate interest in learning about the activities of the government. But the need for a simple rule for public employees has nothing to do with the rights of others who would publish the information or the needs of the public for an informed public discourse. And under ordinary First Amendment standards, those who wish to disseminate such information have the right to do so – unless the government can demonstrate that the publication presents a clear and present danger of grave harm. In this situation, the law arguably *overprotects* the right to publish, as compared to a case-by-case balancing of costs and benefits.

As Justice Stewart observed in the Pentagon Papers case, even though the publication of some of the materials at issue might harm "the national interest," their dissemination could not constitutionally be prohibited unless their dissemination would "surely result in direct, immediate, and irreparable damage to our Nation or its people."²⁶ It is important to note that there are sound reasons for this conclusion.

²⁵ *Id.*, at 727, 728, 730 (Stewart, J., concurring).

²⁶ *Id.*, at 727, 728, 730 (Stewart, J., concurring).

First, the mere fact that dissemination might harm the national interest does not mean that that harm outweighs the benefits of publication.

Second, a case-by-case balancing of harm against benefit would ultimately prove unwieldy, unpredictable, and impracticable. Thus, just as in the government employee situation, there is a compelling need for a clear and predictable rule.

Third, as we have learned from our own history, there are great pressures that lead both government officials and the public itself to underestimate the benefits of publication and overstate the potential harm of publication in times of national anxiety. A strict clear and present danger standard serves as a barrier to protect us against this danger.

And fourth, a central principle of the First Amendment is that the suppression of public speech must be the government's last rather than its first resort in addressing a potential problem. If there are other means by which government can prevent or reduce the danger, it must exhaust those other means before it can suppress the freedom of speech. This, too, is an essential premise of the clear and present danger standard. In the secrecy situation, the most obvious way for government to prevent the danger is by ensuring that seriously damaging information is not leaked in the first place. Indeed, the Supreme Court made this point quite clearly in its 2001 decision in *Bartnicki v. Vopper*,²⁷ in which a radio commentator, received in the mail from an anonymous source a tape recording of an unlawfully intercepted telephone conversation, which the commentator then played on the air. The Court held that the broadcast was protected by the First Amendment, even though the anonymous source could be prosecuted for committing the unlawful wiretap. As the Court explained, when an individual receives information "from a source who has obtained it unlawfully," an individual may not be punished for publicly disseminating even information relevant to public discourse, "absent a need of the highest order."²⁸ The Court reasoned that if "the sanctions that presently attach to [unlawful wiretapping] do not provide sufficient deterrence," then "perhaps those sanctions should be made more severe," but "it would be quite remarkable to hold" that an individual can constitutionally can be punished merely for disseminating information because the government failed to "deter conduct by a non-law-abiding third party."²⁹

V. Conclusion

This is surely a "disorderly situation," but it seems the best possible solution. If we grant the government too much power to punish those who disseminate information useful to public debate, then we risk too great a sacrifice of public deliberation; if we grant the government too little power to control confidentiality "at the source," then we

²⁷ 532 U.S. 514 (2001).

²⁸ *Id.* at 528.

²⁹ *Id.* at 530.

risk too great a sacrifice of secrecy and government efficiency.³⁰ The solution is thus to reconcile the irreconcilable values of secrecy and accountability by guaranteeing *both* a strong authority of the government to prohibit leaks *and* an expansive right of other to disseminate them.

Three questions remain: First, does the same constitutional standard govern criminal prosecutions and prior restraints? Second, what sorts of disclosures might satisfy the clear and present danger standard? And third, how should we deal with information that both satisfies the clear and present danger standard *and* contributes significantly to public debate?

First, in the Pentagon Papers case, the Court emphasized that it was dealing with an injunction against speech. An injunction is a prior restraint, a type of speech restriction that, in the Court's words, bears a particularly "heavy presumption against its constitutionality."³¹ This raises the question whether the test stated in the Pentagon Papers case should govern criminal prosecutions as well as prior restraints.

In dealing with expression at the very heart of the First Amendment – speech about the conduct of government itself – the distinction between prior restraint and criminal prosecution should not carry much weight. The standard applied in the Pentagon Papers case is *essentially* the same standard the Court would apply in a criminal prosecution of an organization or individual for publicly disseminating information about the conduct of government. The clear and present danger standard has never been limited to cases of prior restraint.

Second, is there *any* speech that could constitutionally be punished under this standard? The example traditionally offered was "the sailing dates of transports" or the precise "location of combat troops" in wartime. The publication of such information would instantly make American troops vulnerable to enemy attack and thwart battle plans already underway. Other examples might include publication of the identities of covert CIA operatives in Iran or public disclosure that the government has broken the Taliban's secret code, thus alerting the enemy to change its cipher. In situations like these, the harm from publication might be sufficiently likely, imminent, and grave to warrant punishing the disclosure.

Third, an important feature of these examples often passes unnoticed. What makes these situations so compelling is not only the likelihood, imminence and magnitude of the harm, but also the implicit assumption that these sorts of information do not meaningfully contribute to public debate. In most circumstances, there is no evident need for the public to know the secret "sailing dates of transports" or the secret "location of American troops" on the eve of battle. It is not as if these matters will instantly be topics of political discussion. After the fact, of course, such information may be critical in evaluating the effectiveness of our military leaders, but at the very moment

³⁰ Alexander Bickel, *The Morality of Consent* 79-92 (Yale 1975).

³¹ See 403 U.S., at 730 (Stewart, J., concurring); *id.*, at 737 (White, J., concurring).

the ships are set to sail or the troops are set to attack, it is less clear what contribution the information would make to public debate. My point is not that these examples involve “low” value speech in the conventional sense of the term, but rather that they involve information that does not seem particularly “newsworthy” at the moment of publication, and that this factor seems to play an implicit role in making the illustrations so compelling.

The failure to notice this feature of these hypotheticals can lead to a critical failure of analysis. Interestingly, an analogous failure was implicit in the famous example Justice Holmes first used to elucidate the clear and present danger test – the false cry of fire in a crowded theatre.³² Why can the false cry of fire be restricted? Because it creates a clear and present danger of a mad dash to the exits. Therefore, Holmes reasoned, the test for restricting speech must be whether it creates a clear and present danger of serious harm.

But Holmes’ reasoning was incomplete. Suppose the cry of fire is *true*? In that case, we would *not* punish the speech – even though it still causes a mad dash to the exits – because the value of the speech *outweighs* the harm it creates. Thus, at least two factors must be considered in analyzing this situation – the harm caused by the speech *and* the value of the speech. Suppose, for example, a newspaper accurately reports that American troops in Afghanistan recently murdered twenty members of the Taliban in cold blood. As a result of this publication, members of the Taliban predictably kidnap and murder twenty American citizens. Can the newspaper constitutionally be punished for disclosing the initial massacre? The answer must be “no.” Even if there was a clear and present danger that the retaliation would follow, and even if we agree – as we must – that this is a grave harm, the information is simply too important to the American people to punish its disclosure.

What this suggests is that to justify the criminal punishment of the press for publishing classified information, the government must prove not only that the defendant published classified information, the publication of which would result in likely, imminent and grave harm to the national security, but *also* that the publication would *not* significantly contribute to public debate.

The bottom line is this: The proposed SHIELD Act is plainly unconstitutional. At the very least, it must limit its prohibition to those circumstances in which the individual who publicly disseminates classified information knew that the dissemination would create a clear and present danger of grave harm to the nation or its people.

³² *Schenck v. United States*, 249 U.S. 47, 52 (1919).

Mr. CONYERS. Our next witness is well known here, Abbe Lowell, Esquire, partner at McDermott, Will & Emery. As a matter of fact, he served as chief counsel during the President Bill Clinton impeachment. He is also a former special assistant to the Attorney General, and is well known for his criminal defense work, particu-

larly in espionage matters, including the 2007 AIPAC case. We welcome you back here again, Abbe. You may proceed.

**TESTIMONY OF ABBE DAVID LOWELL, PARTNER,
McDERMOTT WILL & EMERY, LLP**

Mr. LOWELL. Thank you, Mr. Chairman and Judge Gohmert. It is always an honor to be in this particular room. I appreciate you receiving my statement. Let me say that the perspective I bring is, as the Chairman said, comes from basically three points of reference. The first is my service in the Justice Department for the Attorney General when issues of classification were being discussed. The second is 4½ years of litigating under the Espionage Act in the so-called AIPAC lobbyist case that ended 30 days before trial when the Justice Department stopped it and now representing a former Department of State employee also charged under the Espionage Act.

These oversight hearings could not be more important or more timely to look at this principal law that is used whenever cases like the AIPAC lobbyist case and now the WikiLeaks case make the news. However, this law, as everyone has said, is about 100 years old and it had flaws in it in terms of its language from the moment it was passed, and it has certainly shown to be outdated, at least ever since the debate that occurred in the Pentagon Papers case in 1971.

However, as the Chair has said, for all those commentators who are demanding that Congress do something here and now, this Committee knows better that headline news is not the time to pass a new criminal law, especially when there are important constitutional principles at stake, because that inevitably leads to decades of unintended consequences and litigation.

So what this Committee is doing to begin the process of carefully considering these complicated issues is precisely the way to go, and it is the speed in which to travel. Let me start by issuing what I think are the four corners of the discussion. The first is that everyone agrees that there is a need for a strong criminal law to address real spying and espionage, to address the intentional disclosure of what could be called classified national defense information with the intent to injure the United States or to assist an adversary.

There needs to be a law prohibiting the mishandling of properly classified information and against those three important national security principles needs the balance of protecting important constitutional rights. The problem is that the current law lumps all that I have said together, and the sections of the current law apply equally and have been applied equally when they are being used to go after a former FBI agent spy, Robert Hanssen, in disguise in secret in drop zones or two foreign policy analysts having a spaghetti lunch across the river near the Pentagon.

And any law that can apply to those two circumstances is the law that needs to be carefully scrutinized. One more introductory remark, if I may, and this has already been said by everybody across the way from me, when Congress starts deciding how to criminalize the disclosure of classified information, it should take into consideration how much overclassification there really is.

We have seen in the WikiLeaks events material that bear a classification stamp that simply recounts what some diplomat believes is the private life preferences of a foreign leader as opposed to when we are worried about what that foreign leader might do in a military action when properly or improperly provoked, yet they both bear the same classification stamp.

The problems of the law are many. The current law, the Espionage Act particularly, is so vague and so broad because it deals with words that don't have obvious meanings, such as information relating to the national defense, so that they can be applied immediately to a government employee who signs a confidentiality agreement, and then it could be applied to the foreign policy analyst who meets with that government employee and discusses what the government employee knew. And then it could be applied to a reporter who is overhearing the conversation between the government employee and the analyst and prints a story.

Not only that, the current laws can be applied to each of these individuals whether or not there is an actual document involved, or whether the subject of the leak is an oral conversation. And not only that, a prosecution can be brought without the requirement of any of the disclosures involving an actual intent to injure the United States or to assist an adversary. And all this is made more complicated when there are good motives involved, such as somebody trying to bring to the attention of the public a lie the government has stated, or a corrupt contract, or when the press is doing its job or when lobbyists are doing theirs.

Because as the cases state, the First Amendment applies to the exchange of speech and ideas in our free society, whether the information is general foreign policy material or whether it happens to be classified, so the issue is the balancing of the very real and important national security interests of the United States in ever dangerous times.

Over the past few decades, courts have grappled how best to apply the words of the law to these situations. In the AIPAC lobbying case, for example, the court made clear that to sustain a case under the Espionage Act, the government would have to prove beyond a reasonable doubt that the defendants had a specific criminal intent to injure the United States and that they acted in bad faith.

Now that there is the public disclosure of WikiLeaks and Julian Assange, with thousands of documents, these same questions arise again. Does the law apply extraterritorially? Is he or is he not a journalist? Is there the ability to show an intent to injure? All of those are the beginning and not the end. So while the courts are straightjacketed, this Committee in Congress is not, it can operate on a clean slate. And as I have indicated in my statement, let me give you what I think are five principles that any new law should consider: First, we must define spying differently from leaking; second, we need to define what classified information, the release of which can ever be subject to criminal prosecution; third, we must distinguish between disclosures of classified information done with an intent to injure the United States, and those where a person is not acting with that criminal intent; fourth, we must allow for some defense when information is improperly classified or when

that information is so out in the public, that to base a criminal prosecution on it defies the notions of fairness and due process; and last, we need a law that will rationalize how it is possible to apply it to government officials and nongovernment officials, especially when those nongovernment officials are protected by the First Amendment.

That is easier said than done. This is the beginning I know of a long process. I know it is possible to balance those two interests, and along with my panel members, I stand ready to help in any way I can.

Mr. CONYERS. Thank you, Abbe Lowell.

[The prepared statement of Mr. Lowell follows:]

PREPARED STATEMENT OF ABBE DAVID LOWELL

**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, LLP¹**

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 does⁸. 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 country 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.

#

Mr. CONYERS. Our next witness, Kenneth Wainstein, is well known to the Committee as well. He testified here last year. And he also testified as the assistant attorney general on national security. So we welcome him back. He is a partner at O'Melveny & Myers. And he has a particular point of view that the Committee feels is very important that we hear at this time.

**TESTIMONY OF KENNETH L. WAINSTEIN, PARTNER,
O'MELVENY & MYERS, LLP**

Mr. WAINSTEIN. Thank you very much, Chairman Conyers, Judge Gohmert, Members of the Committee. It is an honor to appear before you today along with this panel of very distinguished experts——

Mr. CONYERS. Pull the mic closer to you, please.

Mr. WAINSTEIN. There you go. I missed the on button. I want to thank you again, you, Judge Gohmert, Members of the Committee. It is an honor to appear before you today along with this panel of distinguished experts and to testify about the recent WikiLeaks releases. This situation reflects a fundamental tension in our democracy. On one hand, there is the importance of the free press and the need to think very long and very hard before taking any steps that may chill the media's reporting on the workings of government.

On the other hand, there is the need to keep our national security operations confidential so that we can effectively defend our Nation against the threats it faces. Stephen Vladeck and I testified about this very issue before the Senate Judiciary Committee just this May, and at that time, our concern revolved primarily around the possibility of a leak to a traditional news organization.

Since May, however, we have all learned that there is a much more serious threat, a threat posed by an organization that is committed not to the traditional media function of reporting newsworthy information, but to the mass and indiscriminate disclosure of sensitive information.

Thanks to WikiLeaks the government now has two very important decisions to make. The first is whether to prosecute Assange and WikiLeaks. The second is whether to revise the laws of the Espionage Act to strike a better and clearer balance between security and freedom of the press.

In terms of prosecution, the stakes for the government are very high. If WikiLeaks and Assange end up facing no charges for their mass document releases, which are about as audacious as I have ever heard of, they will conclude that they are legally invulnerable, they will redouble their efforts to match or exceed their recent exploits and copycat operations will sprout up around the Internet.

I was encouraged to hear the Attorney General's remarks the other day, and I commend the Justice Department for apparently undertaking a careful but determined effort to look into mounting a prosecution. If this effort does, in fact, ripen into a criminal case against Assange and WikiLeaks, it will certainly raise a host of hotly litigated issues, the most heated of which will be a strong constitutional challenge under the First Amendment.

The main issue here will be the following: If WikiLeaks can be charged with espionage for these releases, there is no legal and no logical reason why a similar prosecution could not lie against all the other mainstream news organizations because those organizations, at one time or another, published similarly sensitive materials. And if every news outlet in our country is in fear of prosecution then what happens to freedom of the press?

This surely is a serious concern. It is the reason why the government has never prosecuted a news organization for espionage, and

it is the reason that we all should pause and think through the implications before charging into a prosecution here. The key to overcoming this concern is to demonstrate that WikiLeaks warrants this exceptional treatment because it is fundamentally different from other and real media organizations, by showing, for instance, that while the media focuses on disseminating newsworthy information, WikiLeaks focuses, first and foremost, on simply obtaining and disclosing official secrets. While the media gathers news through investigative reporting, WikiLeaks uses encrypted Internet drop boxes that are specifically designed to collect leaked information and circumvent the law. While the media typically publishes only those pieces of sensitive information that relate to a particular story, WikiLeaks indiscriminately releases huge troves of leaked materials.

By clearly showing how WikiLeaks is fundamentally different, the government should be able to demonstrate that any prosecution here is the exception and is not the sign of a more aggressive prosecution effort against the press.

The government's second decision here is whether to revise the Espionage Act. All agree that the statute is badly outdated, and it could use revision on a number of points such as clarifying the level of intent required to prosecute a leak case; determining when the government does and does not need to show that the leak actually risked damage to our national security before proceeding with a case; dropping the term national defense information and providing a clear definition of that information that is protected by the Espionage Act.

A clarification of these issues would go a long way toward making the statute more directly relevant to the espionage threats of the 21st century.

WikiLeaks presents a challenge for the executive branch, which now has to decide how to respond to these disclosures, but it also presents a serious challenge for Congress, which has to decide whether we need new statutory tools to deal with this new threat.

I commend the Committee for stepping up to this challenge. Given the fundamental importance of this issue to our civil liberties and to our national security, I am confident it will be time well spent. I appreciate you including me in this important effort, and I stand ready to answer any questions you may have. Thank you, Mr. Chairman.

Mr. CONYERS. We appreciate you coming before us once again.

[The prepared statement of Mr. Wainstein follows:]

PREPARED STATEMENT OF KENNETH L. WAINSTEIN

STATEMENT OF

KENNETH L. WAINSTEIN
PARTNER, O'MELVENY & MYERS LLP

BEFORE THE

COMMITTEE ON THE JUDICIARY
HOUSE OF REPRESENTATIVES

CONCERNING

THE ESPIONAGE ACT
AND THE LEGAL AND CONSTITUTIONAL
ISSUES RAISED BY WIKILEAKS

PRESENTED ON

DECEMBER 16, 2010

Chairman Conyers, Ranking Member Smith and Members of the Judiciary Committee, thank you for inviting me to this important hearing. My name is Ken Wainstein, and I am a partner at the law firm of O'Melveny & Myers. Prior to my leaving the government in January of last year, I served in a variety of capacities, including Homeland Security Advisor to the President, Assistant Attorney General for National Security, United States Attorney, General Counsel and Chief of Staff of the FBI and career federal prosecutor. It is an honor to appear before you today, along with this panel of very distinguished experts, and to testify about the recent WikiLeaks releases.

This situation reflects the tension in our democracy between protecting government secrets and upholding First Amendment protections for the press. On one hand, it highlights the importance of the free press in our country and the need to avoid interference with its appropriate functioning. An aggressive media is one of the pillars of our democracy, and we need to think long and hard before taking any steps that will chill press efforts to examine and report on the inner workings of government. This concern is particularly strong in regard to news dissemination over the Internet, which has done so much to spread information and knowledge throughout the world and particularly in those countries with repressive governments.

The WikiLeaks releases also remind us of the importance of maintaining the confidentiality of national security deliberations and operations. During my government service, I saw all too often how the failure to do so has debilitating consequences for our policies and national interests. Our military operations and personnel are compromised whenever our adversaries are alerted to our plans; our diplomatic efforts are undermined if foreign counterparts learn how we balance interests and develop negotiating positions; and our Intelligence Community's ability to identify and defeat threats to our Nation is diminished whenever sensitive sources and methods of collection are disclosed.

Congress has long recognized this concern. In fact, Stephen Vladeck and I testified before the Senate Judiciary Committee just this May about the problem of government leaks. At that time, our concern revolved primarily around the leak to a traditional news organization -- the type of leak that has been a fixture of life since the founding of the Republic. Since May, however, we have all learned that there is a much greater threat -- the threat posed by an organization that is committed, not to the traditional media function of reporting newsworthy information, but to the mass and indiscriminate disclosure of sensitive information about the inner workings of our government.

The Challenge of WikiLeaks

This is a threat that far surpasses the age-old problem posed by the news reporter who is tempted to publish a sensitive piece of information that comes his or her way. It arose over the past few years with the development of Internet technology that allows loose, virtual organizations to ferret out government secrets and disclose them in the unconstrained environment of cyberspace with little or no regard to our national security. And, it is a threat that will only get more dangerous with the advance of enabling technology and with the realization after these recent leaks that it takes so little to strike such a grandiose blow against government

secrecy -- nothing more than a computer, access to a disaffected government employee with a clearance, and a willingness to compromise our nation's interests and security.

Given this threat, we now find ourselves at a juncture where the stakes seem much higher than they did when we testified back in May. To the extent the government previously had time for extended deliberation before deciding how to address press leaks, it no longer has that luxury. With their mass disclosures of sensitive information, Julian Assange and WikiLeaks have forced the government's hand.

In responding to that challenge, there are two decisions the U.S. Government needs to make. The first is whether to prosecute Assange and WikiLeaks under our current laws for their mass release of sensitive military and diplomatic documents. The second is whether to revise our current espionage laws to enhance our ability to prosecute, deter and hopefully prevent such damaging leaks in the future. I will address each of these decision points in order.

The Prosecution of Assange and WikiLeaks

There has been much speculation lately about the prospects of successfully prosecuting Assange and WikiLeaks under the Espionage Act -- which is the only type of prosecution I will address today; I won't get into whether these leaks can be charged as a theft of government property or a copyright violation or under some other theory of prosecution.

Assange has professed the belief that he cannot be prosecuted because his conduct is protected by our laws and Constitution. That belief gives him and the other Julian Assanges of the world the sense of security that emboldens them to pursue and disclose government secrets. If Assange and WikiLeaks pay no penalty for their recent audacious releases, that sense of security will become one of invulnerability, they will redouble their efforts to match or exceed their recent exploits, and copycat operations will start to appear throughout the Internet. Just this Tuesday, in fact, a new copycat came on line when a former WikiLeaks employee announced plans to stand up a rival website for leaked materials.

(1) The Legal Issues Arising from a Prosecution

I was heartened to hear the Attorney General's recent statements about holding WikiLeaks accountable for their actions, and I commend the Justice Department for apparently undertaking a careful but determined effort to mount a prosecution. If this effort ripens into a criminal case against Assange and WikiLeaks, it will certainly raise a host of hotly-litigated legal issues.

As an initial matter, the parties will argue over the degrees of malicious intent and damage to the national security that the government will have to show to support an espionage charge. Given that no media organization has ever been brought to trial on leak charges, this is uncharted territory and it is difficult to predict exactly what evidence of intent and national-security damage a court will require before allowing a prosecution to proceed.

Depending on those two threshold legal rulings, there will be a number of challenging factual issues, including the following:

- Whether the released documents could cause actual damage to our national security or are simply embarrassing or awkward for our foreign relations, the latter of which would probably not satisfy any damage element that the court requires.
- Whether Assange's contention that he actually acted out of a salutary desire to provide greater openness and improve our polity would trump the government's ability to demonstrate he intended damage to our national security.
- Whether Assange's pre-release offer to entertain the government's suggested redactions to prevent the release of damaging information undercuts any showing of intent to cause national-security damage.

While these will be difficult issues, it appears from the publicly available information that the government stands a fighting chance of prevailing against the legal challenges and getting its case to the jury. In terms of national-security damage, the best evidence is in those parts of the released documents that discuss and identify persons who have provided information or assistance to our government -- especially those living in the theaters of war whose anonymity is often the key to survival.

In terms of intent, Assange's argument that he meant no harm falters when examined against the record of his actions. While he may well genuinely believe that public access to these materials is good for governance and the governed, he clearly knew that significant injury could result from their release. The documents dealt with some of the most critical matters of state; they contained sensitive information such as the specifics of troop movements and deployments; and lest there was any doubt, the State and Defense Departments put him on notice with letters detailing the damaging consequences that would ensue if he leaked the materials in his possession.

Nor does Assange's claim of complete altruism sound credible in light of some of his recent statements. First, his candid remark that he "enjoy[s] crushing bastards" with his document releases points to a more personal rather than simply a public-minded agenda. Also telling was his recent announcement that further material has been distributed to 100,000 people in encrypted form and that WikiLeaks will decrypt and release key parts of those documents if official action is taken against him. This threat reflects a willingness to use his leaked documents for extortion and personal protection rather than simply to advance the values of transparency and public awareness.

Equally unavailing is his retort that the U.S. Government is to blame for any damage because it rebuffed his offer to entertain proposed redactions. That is a specious argument, and is no different than a burglar claiming innocence because he had previously warned the victimized homeowner to buy an alarm system.

(2) The Primary Constitutional Challenge to the Prosecution

Even if the government prevails in these factual arguments, it will face a strong constitutional challenge based on WikiLeaks' purported media status and the protections afforded the press under the First Amendment. The main issue here is whether prosecuting Assange or WikiLeaks for receiving and disseminating the leaked material -- as opposed to simply prosecuting the responsible government employee for leaking it in the first place -- unduly jeopardizes the constitutionally-protected role of the press in our country. If WikiLeaks can be prosecuted for espionage for these leaks, there is no legal or logical reason why a similar prosecution could not lie against all of the mainstream news organizations that routinely receive and publish protected "national defense information."

I agree that this is a serious concern. It is the reason why we should all pause and think through the implications before charging into a prosecution in this case; it is the reason why the Justice Department has internal procedures for all media-related cases that impose strict limitations on the investigation and prosecution of press activities -- limitations that go well beyond what the law requires; and it is the reason why -- despite the media's publication of leaked classified information on an almost daily basis -- the government has never chosen to prosecute a media organization for espionage.

The key to overcoming this concern is to distinguish WikiLeaks from other news outlets - - to show the difference between WikiLeaks' mission and conduct and the mission and typical conduct of a standard media organization. The main points of distinction are fairly apparent, and include the following:

- The media is generally dedicated to the dissemination of newsworthy information to educate the public; WikiLeaks focuses first and foremost on obtaining and disclosing official secrets.
- The media gathers news about sensitive areas of government operations with probing investigative reporting; WikiLeaks uses its elaborate system of high-security, encrypted drop boxes on the Internet that are designed specifically to facilitate disclosures of sensitive government information and to circumvent the laws prohibiting such disclosures.
- The media typically publishes only those pieces of sensitive information that relate to a particular story of perceived public importance; WikiLeaks is in the business of releasing huge troves of leaked materials with little to no regard for current relevance or resulting damage.

Drawing these distinctions should hopefully lower any First Amendment obstacles to prosecution. It should also reassure the public and media that this case presages no more aggressive prosecution effort against the press and that the Justice Department's longstanding policy of forbearance remains in place for all entities that operate in alignment with the media's traditional purpose and functions.

The Revision of the Espionage Act

The government's second decision is whether and how to undertake a revision of the Espionage Act. As many have recently noted, the statute is badly outdated and in important ways it says both too much and too little. On one hand, the law's broad language suggests that every newspaper reporter who receives a sensitive piece of information relating to the military is subject to espionage prosecution. On the other hand, the law completely overlooks some of our most critical espionage vulnerabilities. While it carefully prohibits the transmission of blueprints and signal books and the use of aircraft to photograph defense facilities, the Espionage Act says nothing about the dissemination of materials over the Internet. Similarly, while there is a whole code section devoted to the disclosure of communications intelligence, the law makes no mention of the disclosure of human intelligence assets.

There are limits to how much the statute can be refined to address every situation. For example, there is probably no practical way -- in this era of diffused and varied means of Internet reporting -- to come up with a definitive list of criteria that can clearly distinguish those entities that qualify as media deserving full First Amendment protection from those that do not. Nonetheless, there are a number of areas where the law could be revised to more clearly delineate the proscribed conduct and better define the relevant standards for prosecution.

A comprehensive review of the Espionage Act should include consideration of the following:

- Clarifying the intent required for prosecuting a government employee who leaks information versus that required for prosecuting the third parties that receive that information.
- Determining when the government needs to demonstrate that the leak caused damage to our national security -- for instance, only when prosecuting the media or also when prosecuting the government leaker -- and defining the potential for damage that is required before a person can be convicted for illegally disclosing information.
- Possibly limiting the reach of the statute to the initial publisher of the leaked materials and not to the person who reads and discusses that publication with others -- as millions have done in the aftermath of the recent WikiLeaks release -- which is arguably considered a separate dissemination and criminalized by the statutes in their current form.
- Dropping the term "national defense information" and providing a clearer definition of the category of information that is protected under the Espionage Act.
- Deciding whether to adopt a law -- as has been proposed -- that would make it unlawful for a government employee to disclose classified information regardless of whether there is potential damage to national security.

While there are numerous other aspects of the Espionage Act that warrant careful review, these are some of the central issues that go to the balance between protecting our official secrets and ensuring freedom of the press. A clarification of these issues will go a long way toward making the statute more directly relevant to the espionage threats of the 21st Century.

* * * * *

WikiLeaks presents a challenge for the Executive Branch, which now has to decide how to respond to these disclosures with the laws that are currently on the books. But, it also presents a challenge for Congress, which has to decide whether we need new statutory tools to sanction and deter egregious releases of government secrets while at the same time maintaining the First Amendment's protections for our free press. I commend the Committee for stepping up to this challenge and for undertaking the complex task of considering revision of the Espionage Act. Given the fundamental importance of this issue to our civil liberties and to our national security, I am confident that it will be time very well spent.

I appreciate you including me in this important effort, and I stand ready to answer any questions you may have.

Mr. CONYERS. I think most people on the Committee are resigned to the fact that we have to look at the Espionage Act in the coming Congress. The question is, of course, what do we do and how much change? We will be talking about that with you when we begin our question period. Welcome, Mr. Schoenfeld, senior fellow at Hudson Institute, a well-known author of *Necessary Secrets: National Secu-*

riety, the Media and the Rule of Law. You have testified in Congress on the responsibilities of the press during wartime, and we welcome you to the Judiciary Committee this morning.

**TESTIMONY OF GABRIEL SCHOENFELD, Ph.D.,
SENIOR FELLOW, HUDSON INSTITUTE**

Mr. SCHOENFELD. Thank you very much, Mr. Chairman, Judge Gohmert, distinguished Members of the Committee. It is an honor——

Mr. CONYERS. I am afraid it is not on.

Mr. SCHOENFELD. It is an honor, Mr. Chairman, Judge Gohmert, distinguished Members of the Committee, to appear here today before you to discuss this issue of such vital concern to our country. The recent massive disclosure by WikiLeaks of U.S. diplomatic documents has sparked the most intense discussion of governmental secrecy in our country since the Pentagon Papers were published by the New York Times in 1971. Leading officials of the Obama administration have decried the damage. Ranking Republicans and Democrats in Congress have called for the prosecution of Julian Assange under the Espionage Act.

Whether or not the Administration takes legal action against Mr. Assange, we should not lose sight of the broader context in which this episode has occurred. And I would like to note several of its significant features. First, we live in the most open society in the history of the world. Thanks in part to an unfettered press and the First Amendment, and thanks in part to laws like the Freedom of Information Act and the Presidential Records Act, we as a country are extremely well informed about what our government does in our name.

Second, even as we are a wide open society, we have too much secrecy. Numerous observers across the political spectrum concur, as we here on the panel seem to be concurring today, that there is a great deal of mis- and overclassification within our national security bureaucracies.

Third, owing in part to mis- and overclassification, the leaking of secret information to the press has become part of the normal informal process by which the American people are kept informed. A study by the Senate Intelligence Committee counted 147 disclosures of classified information that made their way into the Nation's eight leading newspapers in one 6-month period alone. None of these leaks resulted in legal proceedings.

Fourth, many leaks are innocuous and/or authorized. For example, Bob Woodward's recent book, *Obama's Wars*, is replete with code names and descriptions of classified programs. No one has pointed to any specific damage caused by this book, perhaps because the only damage done was to the integrity of the secrecy system itself.

Fifth, some leaks are unauthorized and exceptionally damaging. In 2006, to take one example, The New York Times revealed details of a joint CIA Treasury program to monitor the movement of al Qaeda funds via the Belgium financial clearing house known as SWIFT. The Times published the story against the strenuous objections of leading government officials in both parties.

There is reason to believe that our ability to track the flow of al Qaeda and Taliban funds was severely hampered by the publication of a story that provided few discernible benefits to the public, if any.

So I have sketched here a structure riddled with contradictions. On the one hand, we are a wide open society. On the other hand, we have too much secrecy. On the one hand, we have authorized and innocuous leaks of government secrets. On the other hand, we have unauthorized and highly dangerous leaks.

And this is a very unsatisfactory state of affairs, and we have begun to pay a high price for it. And there are five things we need to do in my judgment, all of them interlinked.

First, we need to devote more attention and resources to declassification to combating overclassification. Fewer secrets and a more rational secrecy policy will help us to preserve truly necessary secrets.

Second, we need to make sure that legitimate whistleblowers have viable avenues other than the media to which they can turn.

Third, we need to reestablish deterrents and prosecute those in government who violate their confidentiality agreements and pass secrets to the press or to an outfit like WikiLeaks. The Obama administration has been doing this with unprecedented energy. The last 24 months have witnessed four prosecutions of leakers, more than all previous presidencies combined.

Fourth, we need, at the very least, to bring down the weight of public opprobrium on those in the media who disseminate vital secrets. In this body, the House of Representatives, contributed to that effort in 2006 when it passed a resolution reprimanding The New York Times and other news organizations for revealing the SWIFT monitoring program.

And finally, we sometimes need to take legal action. We have never had a prosecution of a media outlet in our history, although we came close during World War II when The Chicago Tribune revealed that we had broken Japanese naval codes. Well, I believe that the First Amendment would not protect a news outlet that endangered the Nation as The Chicago Tribune did in 1942. Reasons of prudence suggest that such a prosecution should be a last resort used against the media outlet only in the face of reckless disregard for the public safety.

WikiLeaks, whether it is or is not a news organization, has certainly exhibited such reckless disregard. Thanks in part to the march of technology, it has been able to launch what might be called LMDs, leaks of mass disclosure, leaks so massive in volume and so indiscriminate in what they convey that it becomes very difficult to assess the overall harm precisely because there are so many different ways in which that harm is occurring.

The purpose of these leaks is to cripple our government, which Mr. Assange believes is a "authoritarian conspiracy". But the United States is not such a conspiracy. It is a democracy. And, as a democracy, it has every right to create its own laws concerning secrecy and to see to it that those laws are respected. And as a democracy it has every right to protect itself against those who would do it harm.

Thank you very much for your attention.

[The prepared statement of Mr. Schoenfeld follows:]

PREPARED STATEMENT OF GABRIEL SCHOENFELD

Secrecy in Our Open Society

Hearing of the House Committee on the Judiciary
On the Espionage Act and the Legal and Constitutional Issues Raised by WikiLeaks
Thursday, December 16, 2010

Written Testimony of Gabriel Schoenfeld
Senior Fellow, Hudson Institute, Washington DC,
Resident Scholar, Witherspoon Institute, Princeton, NJ

A basic principle of our political order, enshrined in the First Amendment guarantee of freedom of speech and of the press, is that openness is an essential prerequisite of self-governance. Indeed, at the very core of our democratic experiment lies the question of transparency. Secrecy was one of the cornerstones of monarchy, a building block of an unaccountable political system constructed in no small part on what King James the First had called the “mysteries of state.” Secrecy was not merely functional, a requirement of an effective monarchy, but intrinsic to the mental scaffolding of autocratic rule.

Standing in diametrical opposition to that mental scaffolding was an elementary proposition of democratic theory: Legitimate power could rest only on the *informed* consent of the governed. Along with individuals at liberty to give or to withhold approval to their government, informed consent requires, above all else, information, freely available and freely exchanged. Official secrecy is anathema to this conception. No one has put this proposition more forcefully than James Madison, who tells us that “A popular government, without popular information, or the means of acquiring it, is but a Prologue to a Farce or a Tragedy, or, perhaps both. Knowledge will forever govern ignorance: And a people who mean to be their own Governors must arm themselves with the power which knowledge gives.”

Our country has long operated under a broad consensus that secrecy is antithetical to democratic rule and can encourage a variety of political deformations. Secrecy can facilitate renegade governmental activity, as we saw in the Watergate and the Iran-Contra affairs. It can also be a breeding ground for corruption. Egregious recent cases are easy to tick off.

The potential for excessive concealment has grown more acute as the American national security apparatus expanded massively in the decades since World War II, bringing with it a commensurately large extension of secrecy. In 2008 alone, there were a staggering 23 million so-called “derivative classification” decisions, the government’s term for any step “incorporating, paraphrasing, restating, or generating in a new form information that is already classified.”

With a huge volume of information pertaining to national defense walled off from the public, secrecy almost inevitably has become haphazard. Arresting glimpses of mis- and overclassification are not hard to uncover. The CIA has disclosed, for example, the total government-wide intelligence budget for 1997, 1998, 2007, and 2008, while similar numbers for both intermediate and earlier years remain a state secret. This seems entirely capricious.

Given the massive secrecy, and given our political traditions, it can hardly come as a surprise that leaking is part and parcel of our system of rule. Not a day goes by in Washington without government officials sharing inside information with journalists and lobbyists in off-the-record briefings and in private discussions over lunch. Much of the material changing hands in this fashion winds up getting published. A study by the Senate Intelligence Committee counted 147 separate disclosures of classified information that made their way into the nation’s eight leading newspapers in a six-month period alone.

As these high numbers indicate, leaks to the press are a well-established informal practice. They enable policy makers to carry out any one of a number of objectives: to get out a message to domestic and foreign audiences, to gauge public reaction in advance of some contemplated policy initiative, to curry favor with journalists, and to wage inter- or intra-bureaucratic warfare. For better or worse, leaking has become part of the normal functioning of the U.S. government. And for better or worse, leaking is one of the prime ways that we as citizens are informed about the workings of our government.

But if openness is the default position we would all prefer in a self-governing society, it cannot be unlimited. Secrecy, like openness, is also an essential prerequisite of governance. To be effective, even many of the most mundane aspects of democratic rule, from the development of policy alternatives to the selection of personnel, must often take place behind closed doors. To proceed always under the glare of public scrutiny would cripple deliberation and render government impotent.

And when one turns to the most fundamental business of democratic governance, namely, self-preservation, the imperative of secrecy becomes critical, often a matter of survival. Even in times of peace, the formulation of foreign and defense policies is necessarily conducted in secret. But this is not a time of peace. Ever since September 11, the country has been at war. And we are not only at war, we are engaged in a particular kind of war—an intelligence war against a shadowy and determined adversary. The effectiveness of the tools of intelligence—from the recruitment of agents to the capabilities of satellite reconnaissance systems to the interception of terrorist communications—remains overwhelmingly dependent on their clandestine nature. It is not an overstatement to say that secrecy today is one of the most critical tools of national defense.

The leaking of secrets thus can fundamentally impair our ability to protect ourselves. The various WikiLeaks data dumps of the last few months are a vivid case in point. There is a widespread recognition that the massive releases of classified information have injured the security of the United States. Indeed, thanks in part to the march of technology, we have on our hands what might be called WMDs, weapons of mass disclosure, leaks so massive in volume and so indiscriminate in what they convey, that it becomes difficult to assess the overall harm, precisely because there are so many different ways for the harm to occur. Secretary of State Hillary Clinton has condemned WikiLeaks for “endangering innocent people” and “sabotaging the peaceful relations between nations on which our common security depends.” Admiral Mike Mullen, chairman of the Joint Chiefs of Staff, has stated that WikiLeaks might already have blood on its hands. Secretary of Defense Robert Gates, responding to the release of classified military field reports this past summer, called the

consequences "potentially severe and dangerous" for our troops and Afghan partners.

But the WikiLeaks phenomenon is hardly the only significant and damaging leak of the recent era. To take just one of several examples readily at hand, the 9/11 Commission had singled out the tracking of terrorist finances as one of the weak points in U.S. intelligence that had allowed the Sept 11 plot to succeed. After 9/11, a top secret joint CIA- Treasury Department program was set in motion to monitor the movement of al Qaeda funds via access to the computerized records of a Belgian financial clearing house known as SWIFT. But In June 2006, the *New York Times* published a front-page story revealing the existence of the intelligence gathering effort.

The *Times* story itself noted that the monitoring had achieved significant successes, including providing information leading to the arrest of Hambali, the top operative in that al Qaeda affiliate in Southeast Asia behind the 2002 bombing of Bali in Indonesia. By revealing details of the secret program, the *Times* telegraphed to al Qaeda one of our most important means of tracking its plans. Both leading Republicans and Democrats in Congress, and ranking career intelligence officials said that the leak prompted al Qaeda operatives to move funds in ways far less easy for the U.S. government to track. In this connection, it is quite notable that the al Qaeda and the Taliban are now making extensive use of such means of moving money as untraceable money-grams, hawala, and couriers. Our adversaries do pay attention to what we reveal to them.

The *Times* published the SWIFT story against the strenuous objections of government officials, Republican and Democratic alike. It has never offered a convincing justification for doing so. Its own ombudsman and its chief counsel both subsequently disavowed the decision. Eric Lichtblau, one of the two reporters who wrote the SWIFT story, offered his own rationale for its publication, explaining that it was, "above all else, an interesting yarn." It is difficult to imagine a more trivial justification for a step of such gravity.

Sometimes it takes many years for the damage from such interesting yarns to make itself felt. In my recent book, *Necessary Secrets: National Security, the Media, and the Rule of Law*, I explored an older leak—the so called Black Chamber Affair—that contributed significantly to the success of the Japanese surprise attack on Pearl Harbor. In 1931 a retired American cryptographer by the name of Herbert O. Yardley, out of a job in the Great Depression and having fallen on hard times, published a book called *The American Black Chamber* that laid bare the entire history of American codebreaking efforts, including our prior successes in cracking Japanese codes.

Here in the United States, Mr. Yardley's book was praised highly in some quarters of the press. As one leading publication wrote in a typical vein, "Simply as entertainment, this exposé is well worth the price." In Japan, on the other hand, the book caused an uproar about the laxity with which codes had been constructed. One of the consequences of the uproar was that the Japanese military infused new funds into research on cryptographic security. Within three years they had developed a machine-generated cipher, a precursor to the famously complex Purple code machine. Some sensitive Japanese communications were no longer transmitted over the airwaves even in encrypted form. Instead worldwide courier system was introduced to ensure their secure delivery.

We did not suffer the consequences of any of all this activity for a decade, but in the months before Pearl Harbor, one of the ramifications of Mr. Yardley's book was that the United States was not able to read crucial Japanese military communications, and we missed key warning signs that Pearl Harbor was going to be attacked.

Informing our adversaries of our capabilities is the most direct form of damage caused by leaking. But this hardly exhausts the universe of the kinds of harm that leaks of secret information can cause. Let me mention several others, especially as they impinge today on conduct on the war on terrorism.

For one thing, leaks significantly impact our ability to engage in exchanges of information with allies and adversaries alike. Even routine diplomatic

discourse becomes impossible if both foreign and American officials labor in fear that their confidential remarks are to going to end up on the front page of the *New York Times* via an outfit like WikiLeaks. Even more dangerous is the impact on intelligence sharing. In any particular instance in which information gathered by an ally is particularly sensitive, foreign intelligence officials can be quite reluctant to share it with our government if it will result in a headline that might compromise their own sources and methods, and possibly lead to the deaths of informants and agents.

For another thing, leaks tend to cripple our deliberative and decision-making processes. We have vast national-security bureaucracies filled with leading experts on all manner of questions. And yet whenever important decisions are taken, ranking officials almost always conclude that it essential to push their underlings away as far as possible, lest someone in the bowels of the bureaucracy, for whatever motive, places a telephone call to a reporter and torpedoed the policy. American decisionmakers are thus compelled to take crucial decisions while in effect groping in the dark, with results that often times speak for themselves.

And for yet another thing, leaks constrict the arteries by which information is circulated across and within the national- security machinery of the U.S. government. The 9/11 Commission pointed to a dearth of information sharing among government agencies as one of the factors that led to al Qaeda's terrible achievement in penetrating our defenses. Remedial measures taken after September 11 have allowed information to flow more freely to where it needs to go, although bottlenecks still exist. The Pentagon, for its part, has succeeded in pushing raw intelligence down to the war-fighters on the battlefield so that it can actually be used. But with greater access came greater risks. One of those risks turned up in the person of Pfc. Bradley Manning, who seems to be the culprit who turned over vast quantities of information to WikiLeaks. That breach has increased the pressure to tighten the information spigot, undoing some of the important gains in our counterterrorism efforts garnered by post 9/11 reforms.

Finally, leaking is an assault on democratic self-governance itself. We live in a polity that has an elected president and elected representatives. Leaking is a way in which individuals elected by no one and representing no one can use their privileged access to information to foist their own views on a government chosen by the people.

There are two different kinds of perpetrators engaged in this assault and they operate under very different ethical and legal strictures. On one side are so-called whistleblowers, who pass along secrets from within the national-security apparatus to journalists. Somewhere upward of 2.4 million Americans hold security clearances. A population that size will always contain a significant quotient of individuals disaffected for one or another reason. The power to leak on a confidential basis offers any one of the 2.4 million a megaphone into which he or she can speak while wearing a mask. Often acting from partisan motives or to obtain personal advancement, and almost always under the cover of anonymity, such whistle-blowers are willing to imperil the nation but not their careers.

The other face of the assault on democratic self-government comes from journalists, who operate in tandem with the whistleblowers, and claim protection to publish whatever they would like under the banner of the First Amendment. In publishing leaked materials, journalists indefatigably demand openness in government and claim to defend the people's "right to know." But along with the public's "right to know," constantly invoked by the press, there is also something rarely spoken about let alone defended: namely the public's right *not* to know. Yet when it comes to certain sensitive subjects in the realm of security, the American people have voluntarily chosen to keep themselves *uninformed* about what their elected government is doing in their name. The reason why we choose to keep ourselves uninformed is not an enigma. It is obvious. We entrust our government to generate and to protect secrets, secrets that are kept from us, because what we know about such matters our adversaries will know as well. If we lay our secrets bare and fight the war on terrorism without the tools of intelligence, we will succumb to another attack.

Norman Pearlstine, the chief executive of Time Inc, says that “when gathering and reporting news, journalists act as surrogates for the public.” Pearlstine’s observation can be true. But when journalists reveal secrets necessary to secure the American people from external enemies, a converse observation can be true. In that event, journalists are not surrogates for the public but usurpers of the public’s powers and rights.

Reporters and editors regard themselves as public servants, but they suffer from a tendency to forget that they are private individuals, elected by no one and representing no one. They operate inside private corporations which are themselves not at all transparent. Indeed, the putative watchdogs of the press, ever on the lookout for the covert operations of government, can themselves be covert operators, with agendas hidden from the public. The press plays an indispensable role in our system as a checking force, but its practitioners can and sometimes do wield their power—including the power to disclose government secrets—for political ends of their own choosing.

That is not the only point of conflict between the press and the public, for newspapers are also profit-seeking institutions. Every day of the year, journalists delve into the potential and real financial misdeeds and conflicts of interest besetting corporate America. But newspapers, curiously, seldom if ever delve into the potential and real conflicts of interest besetting journalism, particularly in the area of publishing sensitive government secrets. Or perhaps it is not so curious. For journalists operate inside a market economy in which financial rewards accrue not just to news corporations and their shareholders but also to they themselves. A Pulitzer Prize brings immense prestige in the profession, and a \$10,000 check, a sum almost always matched by news organizations with generous raises and/or bonuses. And then of course there is a book market in which discussion of secret programs can generate hundreds of thousands of dollars in royalties. Lecture fees can add tens of thousands of dollars more. The incentives to cast aside scruples about injury to national security, injury that is seldom immediately apparent, and lay bare vital secrets can be powerful, indeed, irresistible.

At the end of the day, we are presented with two conflicting positions: on the one hand, leaking is a necessary and widespread practice inside our democracy. On the other hand, it is fundamentally anti-democratic and it can cause great harm. Both views are right and we are faced with a contradiction. How can the tension between these two very different faces of the phenomenon be reconciled?

One pathway through the contradiction is by looking at the legal framework in which the leaking occurs. For law is not just a mechanical set of rules and sanctions, but also a moral code by which conduct can be considered and judged.

There are two classes that have to be considered here: leakers and those who disseminate information provided by the leakers to a mass audience.

Leakers are almost in every instance, except when they possess the actual legal authority to declassify information, breaking the law. Everyone who works with classified information is in effect being entrusted by the public to safeguard the secrets they encounter. As a condition of employment, they are asked to sign an agreement pledging to observe the laws protecting those secrets. The agreement reads in part:

I have been advised that the unauthorized disclosure, unauthorized retention, or negligent handling of classified information by me could cause damage or irreparable injury to the United States or could be used to advantage by a foreign nation. I hereby agree that I will never divulge classified information to anyone unless: (a) I have officially verified that the recipient has been properly authorized by the United States Government to receive it; or (b) I have been given prior written notice of authorization from the United States Government Department or Agency (hereinafter Department or Agency) responsible for the classification of the information or last granting me a security clearance that such disclosure is permitted. I understand that if I am uncertain about the classification status of information, I am required to confirm from an authorized official that the information is unclassified before I may

disclose it, except to a person as provided in (a) or (b), above. I further understand that I am obligated to comply with laws and regulations that prohibit the unauthorized disclosure of classified information. ... I have been advised that any unauthorized disclosure of classified information by me may constitute a violation, or violations, of United States criminal laws.

Nothing about this promise is unclear. No one who affixes his name to this nondisclosure agreement is compelled to do so; government officials sign it of their own free will.

What is more, officials who uncover illegal conduct in the government are by no means bound by their signature to keep silent and permit violations of law to continue. Congress has enacted “whistleblower protection acts” that offer clear and workable procedures for civil servants to report misdeeds and ensure that their complaints will be duly and properly considered. When classified matters are at issue, these procedures include direct appeals to the Justice Department and to members of the intelligence committees in Congress. They emphatically do not include blowing vital secrets by disclosing them to al Qaeda and the rest of the world via WikiLeaks or the news media.

The rules and laws governing leakers are quite clear. The same, alas, cannot be said regarding those who disseminate leaked information in the media. Here there are two radically opposing views.

On one side there is the position put forward by journalists, who maintain that the First Amendment gives the press an absolute right to publish whatever government secrets it wants to publish. Bill Keller, executive editor of the *Times*, says that the Founding Fathers, in opening the Bill of Rights with the First Amendment, “rejected the idea that it is wise, or patriotic to surrender to the government important decisions about what to publish.” This absolutist view of the First Amendment is widespread among journalists. They say that the words of the First Amendment are unequivocal: “Congress shall make no law . . . abridging the freedom of speech, or of the press.” “No law” means “no law,” are what journalists and their defenders repeat over and over again.

But the framers were hardly the apostles of libertarianism that they are today made out to be by Mr. Keller and many others. More than anything else, the First Amendment was conceived of by the framers as a continuation of the Blackstonian understanding embedded in British common law, as a prohibition on prior restraint on the press. Censorship was what the framers aimed to forbid. But laws punishing the publication of certain kinds of material after the fact were something else again. Joseph Story, the preeminent 19th century interpreter of the Constitution put this understanding most forcefully when he wrote that the idea that the First Amendment was “intended to secure to every citizen an absolute right to speak, or write, or print, whatever he might please is a supposition too wild to be indulged by any rational man.”

And indeed our courts have long held, and the press itself has long readily accepted, that the sweeping words of the First Amendment are fully compatible with legal restrictions on what journalists can and cannot say in print. Statutes forbidding certain kinds of commercial speech and punishing libel, to which virtually no one inside the media ever objects, have long been held to be fully constitutional abridgements of freedom of the press.

But in the vital area of national security, journalists nevertheless insist that they and they alone are the final arbiters of what can and cannot be published. And they act upon this insistence, publishing national-security secrets on some occasions with little or no regard for the consequences. As Dean Baquet, the Washington bureau chief of the *New York Times*, has put it, the press is free to publish whatever it wishes “no matter the cost.”

But Mr. Baquet’s understanding is not in line with either our Constitution or our laws. Congress—that is, the American people, acting through their elected representatives—has enacted a number of different statutes that prohibit the publication of certain kinds of national-security secrets. Thanks to the Valery Plame-Judith Miller affair, we are most familiar these days with a 1982 law, the Intelligence Identities Protection Act, that makes it a felony to disclose the identity of undercover operatives working for the CIA or other U.S. intelligence agencies. Congress has also carved out special protection for secrets concerning

atomic weapons and communications intelligence. The 1917 Espionage Act offers a more general blanket protection to all closely held information pertaining to national defense.

These laws are on the books, and they have been upheld by the Supreme Court. But the stark fact is that they are not being enforced. Remarkably enough, despite how ubiquitous leaking is in our system—there have been only three successful prosecutions of leakers in our entire history. The prosecution of leakers is rare because they are exceptionally difficult to catch. Almost every president beginning with Richard Nixon has launched investigations designed to ferret out leakers, but law enforcement almost always comes up empty. The simple fact is that typically with respect to any given leaked secret, too many people, sometimes hundreds, have had access to it, and the tools of investigation, including polygraph interviews, simply do not yield results. The problem of controlling the illicit flow of information out of the bureaucracies remains unresolved.

As for prosecutions of the press, they have been rarer still than the prosecution of leakers. Indeed, there have been no successful convictions in our entire history and only one attempted prosecution. That attempted prosecution occurred during World War II, and is highly relevant today. It was directed against the *Chicago Tribune*, then published by Colonel Robert McCormick, an ardent isolationist, who seemed to hate Roosevelt far more than he hated either Hitler or Hirohito.

In 1942, in the immediate aftermath of the Battle of Midway, the *Chicago Tribune* published a story strongly suggesting that the decisive American naval victory at Midway owed to the fact that the United States had been successfully reading Japanese codes. Shocked officials in the War Department in Washington sought to throw the book at Col. McCormick and a grand jury was empanelled to hear evidence and bring charges. When it turned out that the Japanese had not changed their codes in reaction to the news story, the War Department asked the Justice Department to drop the proceedings lest further attention be called to a story the Japanese had seemingly ignored.

But there can be no blinking the gravity of that breach. If the United States, thanks to the *Chicago Tribune*, had lost its window into Japanese military communications, the war in the Pacific would still have ended in certain Japanese defeat. That outcome was all but assured by the atomic bomb. But three years were to elapse before the atomic bomb was ready for use. In the interim, without the priceless advantage of knowing Tokyo's every next move in advance, thousands—tens of thousands—of American soldiers and sailors would have needlessly died.

Since 1942, we have never had a subsequent prosecution. Perhaps the major reason is that the press has for the most part, until quite recently, been fairly restrained and responsible. Consider, for example, the *New York Times*'s decision in 1971 to publish excerpts of the top-secret collection of documents provided to it by Rand Corporation researcher Daniel Ellsberg. By any measure, that was the most sensational leak in all of American history up to its time. But the Pentagon Papers case was sensational not so much because of the sensitive nature of the secrets disclosed but primarily because Richard Nixon tried, unsuccessfully, to get a prior restraint from the courts to stop the presses.

In the Pentagon Papers case, the secrets at issue were nothing at all like the ultra-sensitive material published by the *Chicago Tribune*. The Pentagon Papers became public during the Nixon administration, but they had been compiled during the Johnson administration. By 1971, when Mr. Ellsberg turned the Pentagon Papers over to Neil Sheehan of the *New York Times*, not one of the documents in the Pentagon Papers case was less than three years old. Though the documents bore a top-secret stamp, the passage of time had rendered them nearly innocuous. No ongoing intelligence operations or war plans were disclosed.

This brings us back to our current dilemmas. For the fact is that the material being published today by WikiLeaks and by our leading newspaper is closer to what the *Chicago Tribune* published during World War II than to what was contained in the Pentagon Papers. The secrets that are being revealed today are not historical in nature; they involve ongoing diplomatic, military and intelligence programs.

Such conduct brings urgently to the fore a fundamental question raised by the phenomenon of leaking: namely, who in the final analysis gets to decide what can be kept secret and what cannot?

It is not question susceptible to a glib answer or an easily formulated rule, for the crux of the matter is that the public interest in transparency, and a vigorous press that ensures transparency, is diametrically opposed to the public interest in secrecy.

On the one hand, we live now in a world in which small groups of remorseless men are plotting to strike our buildings, bridges, tunnels, and subways, and seeking to acquire weapons of mass destruction that they would not hesitate to use against our cities, taking the lives of hundreds of thousands or more. To contend with that grim reality, our national-security apparatus inexorably generates more secrets, and more sensitive secrets, and seemingly exercises weaker control over those same vital secrets than ever before.

Yet on the other hand, we cannot lose sight of facts that I noted at the outset, namely, that our national security system is saddled with pervasive mis- and overclassification that remains entrenched despite universal recognition of its existence and numerous attempts at reform.

With the two desiderata of set in extreme tension, it would hardly make sense for the Justice Department to prosecute the press on each and every occasion when it drops classified information into the public domain. Such an approach would be absurd, a cure that would drain the lifeblood from democratic discourse and kill the patient.

A much more reasonable approach would be to continue to live with the ambiguities of our current practices and laws. Vigorously prosecuting and punishing leakers is an obvious place to begin. It is an irony that it is Barack Obama, the President who came into office pledging maximum transparency in government, who is now carrying out such a policy. His administration has thus

far launched four leak prosecutions, more than all preceding American presidents combined.

As for the press, a first step is to try to alter the political climate in which irresponsible tell-all-and-damn-the-consequences journalism flourishes. The WikiLeaks case, in which documents have been released wholesale with consequences that cannot yet even be imagined, has already caused a change in attitudes, making it clear to the public that not all so-called whistle-blowing is commendable, and that in extreme cases, the dissemination of secrets can merit prosecution.

The press does and should have an essential checking role on the government in the realm of foreign affairs, national defense, and intelligence. And that checking role, if it is to be more than a charade, must extend, as it now does, into the inner workings of the U.S. national security apparatus where secrecy is the coin of the realm. But in ferreting out and choosing to report secrets, the press has to exercise discretion.

Newspaper editors are fully capable of exercising discretion about sensitive matters when they so choose. A dramatic example came to light in 2009 when the *New York Times* revealed that it had succeeded for a period of six months in suppressing news that one of its reporters, David Rohde, had been kidnapped in Afghanistan by the Taliban. Indeed, the editors seemed to exercise the art of concealment with greater success than the U.S. government's own secrecy apparatus is often capable of achieving. Neither the *Times* nor its industry competitors, who readily agreed to gag themselves at the *Times*'s request, published a word about the missing journalist until Mr. Rohde escaped his captors and made his way to safety. Bill Keller's explanation was: "We hate sitting on a story, but sometimes we do. I mean, sometimes we do it because a military or another government agency convinces us that, if we publish information, it will put lives at risk."

Mr. Keller deserves some measure of praise for that. But such discretion cannot be—and under our current laws is not—a strictly voluntary affair. Despite Mr. Keller's claims, the *Times* and other leading newspapers have been

far from responsible in their handling of secrets. But even if they were models of rectitude, the public would still be left without recourse in the face of other lesser publications that are not such models, or outfits like WikiLeaks.

Thus, even as the press strives to carry the invaluable function of delving into government secrets, this does not mean it should be exempt from the strictures of law. What it does mean is that in enforcing the law, the executive must also exercise judgment and seek to punish only the publication of those secrets that truly endanger national security while giving a pass to all lesser infringements.

Just as there must be editorial discretion, so too must there be prosecutorial discretion. It is right and proper that jaywalkers are not ticketed for crossing little-trafficked roads. It is also right and proper that they are arrested for wandering onto interstate highways. When newspaper editors publish secrets whose disclosure is arguably harmless—say, for example, the still-classified CIA budget for fiscal year 1964—or secrets that conceal abuses or violations of the law, they should trust that, if indicted by a wayward government, a jury of twelve citizens would evaluate the government’s ill-conceived prosecution and vote to acquit. On the other hand, if newspapers editors or an organization like WikiLeaks disclose a secret vital to our national security—and have no justification for doing so beyond a desire to expose for exposure’s sake—they should also be prepared to face the judgment of a jury of twelve citizens and the full wrath of the law. Journalists and their defenders, and WikiLeaks and its defenders, find that view anathema. They want unlimited freedom and accountability to no one but themselves. Their behavior raises the fundamental question of whether the free society built by the Founding Fathers can defend itself from those who would subvert democracy by placing themselves above or outside the law.

I thank the members of the Committee for addressing the difficult and important issues involved in maintaining secrets in an our open society.

Mr. CONYERS. Thank you so much, Mr. Gabriel Schoenfeld.

Our next witness, Professor Steve Vladeck, is professor of law at American University. He was part of the legal team that successfully won *Hamdan v. Rumsfeld*, challenging former President George W. Bush’s use of military tribunals. He is well-known to the judiciary; and as the WikiLeaks controversy has unfolded, he has

further distinguished himself as one of the foremost national experts on the matter.

We welcome you here.

**TESTIMONY OF STEPHEN I. VLADECK, PROFESSOR OF LAW,
AMERICAN UNIVERSITY**

Mr. VLADECK. Thank you, Mr. Chairman.

Chairman Conyers, Judge Gohmert, distinguished Members of the Committee, thank you very much for inviting me to participate in this important hearing. I hope my testimony won't sound too much like a broken record.

You know, testifying before the House Permanent Select Committee on Intelligence in 1979, Tony Lapham, who was then the general counsel of the CIA, describes the uncertainty surrounding the scope of the Espionage Act 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 discussion 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 statute benefits no one and leaves many questions unanswered about who may be held liable and under what circumstances, for what types of conduct.

In my testimony today I would 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.

First, as the title suggests and as Mr. Lowell testified, 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 its specific intent either to harm the national security of the United States or 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 power.

No separate statute, as this Committee knows, 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 view of the merits, I very much doubt that the Congress that drafted the Espionage Act in the midst of the First World War meant for it to cover each of these categories, let alone 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.

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 that Mr. Lowell testified about, read into the Espionage Act a second mens rea. As he explained, whereas the statute's willfulness requirement obligates the government to prove that defendants know that disclosing documents could threaten national security, and that it is 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 the 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. In other words, courts have basically stumbled around to try to mesh the First Amendment concerns with the very vague and sweeping language of the statute.

Fourth, and briefly, the potentially sweeping nature of the Espionage Act as currently written may inadvertently interfere with Federal whistleblower laws. For example, the Whistleblower Protection Act 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 secret in the interest of national defense or the conduct of foreign affairs. Similar language appears in most other Federal whistleblower statutes.

I daresay the government would be reluctant to prosecute an individual who complied with Federal whistleblower laws, but I think that the statute could be amended to remove that within the realm of possibility.

And, finally—I won't even talk about this in detail, because it was already been mentioned by my colleagues—the problem of overclassification. Should there be a defense for improper classifica-

tion? How do we actually attack the real elephant in the room when we are talking about the disclosure of things that perhaps should never have been kept secret in the first place?

What is to be done. Perhaps unsurprisingly in light of my observations above and those of my colleagues, I would recommend three distinct sets of changes to the Espionage Act:

First, 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 harm national security and/or to benefit a foreign power. I think you have already heard this from Mr. Lowell.

Second, create a separate, lesser offense for unauthorized disclosures and retention of classified information and specifically provide either that such a prohibition does or does not cover the public redistribution of such information, including by the press. If this Committee and body does decide to include press publication, my own view is that the First Amendment requires the availability of any number 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.

Third, and finally, 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.

Mr. Chairman, in summation, writing in a Law Review article about 40 years ago, Hal Edgar and Benno Schmidt, two Columbia Law School professors, wrote that “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 last 40 years and, if recent events are any indication, increasingly less benign.

Thank you for the invitation to testify. I look forward to your questions.

[The prepared statement of Mr. Vladeck follows:]

PREPARED STATEMENT OF STEPHEN L. VLADECK

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 L. 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.

Mr. CONYERS. Well, you have left us with some very large challenges, Professor Vladeck. We appreciate it very much.

Our next witness is the Director of the National Security Archive at George Washington University, Professor Thomas Blanton. In the year 2000, the Archive won the George Polk award for “piercing self-serving veils of government secrecy, guiding journalists in

search of the truth and informing us all.” He is also the founding editorial board member of freedominfo.org, a network of international freedom of information advocates.

I read your prepared statement with great enthusiasm, and we are happy to have you here today.

TESTIMONY OF THOMAS S. BLANTON, DIRECTOR, NATIONAL SECURITY ARCHIVE, GEORGE WASHINGTON UNIVERSITY

Mr. BLANTON. Mr. Chairman, it is a great honor for me, and Judge Gohmert and also to be in the middle of this extraordinary high-level tutorial in the Espionage Act and the Constitution. I feel like a grad student again; and it is a joy, actually.

I also wanted to thank you, Mr. Chairman, for resurrecting my graveyard quote, that we have low fences around vast prairies of government secrets where we really need tall fences around small graveyards of the real secrets; and that is a core point I want to come back to today.

I really have three points. One of them is the government always overreacts to leaks, always; and all you have to do is say the phrase “Watergate plumbers” and you know what I am talking about.

Back then, they were discussing firebombing the Brookings Institution on the chance there might still be a copy of the Pentagon papers in there. Today, you are having debates on FOX news: Let’s do some targeted assassination attempts on Julian Assange.

Well, I have to say G. Gordon Liddy would be right at home, and both is absurd. And the overreaction the government typically does is not to kill anybody or to firebomb something but to go right to the second major point I want to make today. They are going to classify more information.

What I am worried about most is the backlash. I mean, in my prepared statement, I have got multiple examples of all the estimates, and they range from 50 percent to 90 percent, of what the problem of overclassification really amounts to. Governor Tom Kean, head of the 9/11 Commission, after looking at all of the al Qaeda intelligence that we gathered before 9/11, said, you know, 75 percent of what I saw that was classified should not have been. And the Commission said we not only needed to do information sharing between the agencies, we had to do information sharing with the American people, because that is the only way we can really protect ourselves. What a great lesson that is.

The system is so overwhelmed with the secrets that we can no longer really protect the real ones and we can’t let out the ones that would actually keep us all safer.

And I think it is a mistake to try to see this as a balancing test. It is not a balance between openness and security. The findings of the 9/11 Commission were that more openness would have made us more secure. That is what you do in an open society to keep yourself safe. You are not safer in the dark. You don’t hide your vulnerabilities. You expose them and you fix them. That is how we proceed in America.

The third point I just want to make about where we are today. We are in the middle of a syndrome that one senior government official I really respect holds all the clearances, does the audits,

pushes back against excessive secrecy, called it Wikimania. We are in the middle of Wikimania, and it is going to lead to so much more heat than light. Targeted assassination is only the most extreme case, but look at all the other proposals we have got on the table and the front burners to try to push back, to punish WikiLeaks, to push back against speech.

I think the problem here is we have got to look at each one of those proposals and say, is that really going to address the problem? Is it going to reduce government secrecy or is it going to add to it? Is it going to make us more safe? Is it going to make us more free? And do that test.

The Wikimania is really coming from a series of what in my statement I call Wikimyths. There has not been a documents dump. Everybody uses that phrase. There hasn't been one. The less than 2,000 cables are on the public record today out of that big database, and the editors of Le Monde and the Guardian and New York Times say that WikiLeaks is consulting with them about what to publish, what to redact and doing the dialogue with government officials in a pretty extraordinary, responsible way.

It is a very different posture, I should say, than WikiLeaks had even 6 or 8 months ago. I think the criticism they have gotten from journalists like us and from the public about endangering people's lives in Afghanistan and elsewhere, believe it or not, I think they have actually heard it.

There is no epidemic of leaks. In fact, all four of the big WikiLeaks publicity spats have come from a single person as far as we know, Bradley Manning, a young private.

So how do you solve the Bradley Manning problem? Well, you could do a pretty simple thing. The Defense Department has already done it. And here is a rational security policy. Just like you got two people to launch nuclear missiles, you have got two people to handle a communications manual that has codes in it, have two people before you can download something from a secure network. Pretty simple. That would have stopped Bradley Manning. Mormons send out two people as missionaries because that is how you have accountability, right? You don't have solos. All right.

There is no diplomatic meltdown from the WikiLeaks. I mean, there is a lot of heated rhetoric. But Secretary of Defense Robert Gates who ought to know—he served every President in my lifetime, as far as I can tell—and, Mr. Chairman, you quoted his remarks. Yeah, it is awkward, yeah, it is embarrassing, but, no, it is not a meltdown. It will make the job harder for diplomats. Maybe somebody is going to have to be reassigned. But, you know, in the long run, it is probably in the American national security interest for more foreign governments to be more accountable to their own citizens for their diplomacy. It is probably in our national security interest for the King of Saudi Arabia to actually be on the public record a little more often and the China politburo members to get exposed every now and then. That might be a long-term goal of what American national security diplomacy ought to be about.

And, finally, there is not a set of Wiki terrorists. I have heard that phrase batted around. They are not terrorists.

I have to tell you, I wish every terrorist group in the world would write the U.S. ambassador in their local town, you know, days or

a week before they are about to launch something, and ask the ambassador, hey, would you help us, you know, make sure nobody innocent gets hurt? Would you really work with us? We would be glad to talk to you.

And I understand why the ambassadors didn't believe them. Because WikiLeaks said, oh, and, by the way, we will keep anything you say to us confidential. It is hard to square with the previous statements of WikiLeaks.

But I wish every terrorist group would get into partnership with Le Monde and El Pais and the Guardian and the New York Times to assess what the damage might be, to redact their own documents, to put regulators on the bombs they drop. That would be a good thing. WikiLeaks is not terrorists.

And so that brings me to my final real point and recommendation to this Committee and to the prosecutors across the river in Alexandria: Just restraint. I know you don't usually have witnesses come up here and say, hey, let's all go take a nap. But you know in sleep-deprived Washington we might could use a little more restraint.

I would say leave the Espionage Act back in mothballs where it is right now and should stay. And in fact what we know is from some freedom of information requests there are still some classified documents from 1917 that will give the Espionage Act very good company. Don't mess with it. Leave it alone.

Our fundamental test should come out of Justice Stewart's dicta in the Pentagon papers case and some wonderful articles that Jack Goldsmith has actually written in the last couple of years where he says, look, our problem is, you know, the fundamental cause of leaks is a sense of illegitimacy that is bred by excessive government secrecy.

How do you address that? You reduce the secrecy. How do you deal with the legitimacy problem? You make sure as few secrets as possible are actually held and you protect those very strongly.

So the test is, for all these proposals, legislative and otherwise, does it send a signal that will actually reduce government secrecy? Does it send a signal that we need maximum possible disclosure, in Stewart's phrase, to have a system that actually has credibility and can protect the real secrets and where we can protect ourselves?

I thank you, Mr. Chairman, for this opportunity to engage in this debate. I hope it will reduce the mania a little bit and cut through some of the myths. Thank you, sir.

[The prepared statement of Mr. Blanton follows:]

PREPARED STATEMENT OF THOMAS S. BLANTON

Statement of Thomas Blanton
Director, National Security Archive, George Washington University
www.nsarchive.org

To the Committee on the Judiciary
U.S. House of Representatives

Hearing on the Espionage Act and the Legal and Constitutional
Implications of Wikileaks

Thursday, December 16, 2010
Rayburn House Office Building, Room 2141
Washington D.C.

Mr. Chairman, Ranking Member Smith, and members of the Committee, thank you for your invitation to testify today on the implications of the Wikileaks controversy. I am reminded of the ancient Chinese curse, "May you live in interesting times."

I have three main points to make today:

First, the government always overreacts to leaks, and history shows we end up with more damage from the overreaction than from the original leak.

Second, the government's national security classification system is broken, overwhelmed with too much secrecy, which actually prevents the system from protecting the real secrets. The rest should all come out.

Third, we are well into a syndrome that one senior government official called "Wikimania," where Wikimyths are common and there is far more heat than light – heat that will actually produce more leaks, more crackdowns, less accountable government, and diminished security.

By way of background, I should say right up front that my organization, the National Security Archive, has not gotten any 1.6 gigabyte thumb drives in the mail in response to our many Freedom of Information Act requests, nor have we found any Bradley Mannings among the many highly professional FOIA officers who handle our cases. It's a lot more work to pry loose

national security documents the way we do it, but then it's a lot of work worth doing to make the rule of law a reality and give real force to the Freedom of Information Act.

It takes us years of research and interviews and combing the archives and the memoirs and the press accounts, even reading the agency phone books, to design and file focused requests that don't waste the government's time or our time but hone in on key documents and key decision points, then to follow up with the agencies, negotiate the search process, appeal the denials, even go to court when the stonewalling gets out of hand. Changing the iron laws of bureaucracy is a tall order, but we have allies and like-minded openness advocates in more than 50 countries now, passing access laws and opening Politburo and military dictators' files, poring through Communist Party records and secret police archives and death squad diaries, rewriting history, recovering memory, and bringing human rights abusers to trial.

Our more than 40,000 Freedom of Information requests have opened up millions of pages that were previously classified; we've published more than a million pages of documents on the Web and other formats; our staff and fellows have authored more than 60 books, one of which won the Pulitzer. Our Freedom of Information lawsuits have saved tens of millions of White House e-mail spanning from Reagan to Obama, whose Blackberry messages are now saved for posterity.

The George Foster Peabody Award in 1998 recognized our documentary contributions to CNN's *Cold War* series both from the Freedom of Information Act and from the Soviet archives; the Emmy Award in 2005 recognized our "outstanding achievement in news and documentary research"; and the George Polk Award citation (April 2000) called us "a FOIL'ers best friend" and used a wonderful phrase to describe what we do: "piercing the self-serving veils of government secrecy, guiding journalists in search for the truth, and informing us all."

Most pertinent to our discussion here today is our experience with the massive overclassification of the U.S. government's national security information. Later in this testimony I include some of the expert assessments by current and former officials who have grappled with the secrecy system and who estimate that between 50% to 90% of what is classified is either overclassified or should not be classified at all. That reality should restrain us from encouraging government prosecutors to go

after anybody who has unauthorized possession of classified information: such encouragement is an invitation for prosecutorial abuse and overreach – exactly as we have seen in the case of the lobbyists for the American Israel Public Affairs Committee.

The reality of massive overclassification also points us towards remedies for leaks that are the opposite of those on the front burners such as criminalizing leaks. The only remedies that will genuinely curb leaks are ones that force the government to disgorge most of the information it holds rather than hold more information more tightly.

But a rational response to excessive government secrecy will be even more difficult to achieve in the current atmosphere of Wikimania. The heated calls for targeted assassinations of leakers and publishers remind me of the Nixon White House discussions of firebombing the Brookings Institution on suspicion of housing a copy of the Pentagon Papers. It was the earlier leak of the secret bombing of Cambodia that started President Nixon down the path to the Watergate plumbers, who began with righteous indignation about leaks, then moved to black bag jobs and break-ins and dirty tricks, and brought down the presidency. All the while, as the Doonesbury cartoon pointed out, only the American people and Congress were in the dark. One famous strip showed a Cambodian couple standing amid bomb wreckage, and the interviewer asks, was this from the secret bombing? Oh, no, not a secret at all, “I said, look Martha, here come the bombs.”

Few have gone as far as Nixon, but overreaction to leaks has been a constant in recent American history. Almost every president has tied his White House in knots over embarrassing internal leaks; for example, the moment of greatest conflict between President Reagan and his Secretary of State George Shultz was not over the Iran-contra affair, but over the idea of subjecting Shultz and other high officials to the polygraph as part of a leak-prevention campaign. President Ford went from supporting to vetoing the Freedom of Information Act amendments of 1974 because of his reaction to leaks (only to be overridden by Congress). President George W. Bush was so concerned about leaks, and about aggrandizing presidential power, that his and Vice President Cheney’s top staff kept the Deputy Attorney General, number two at Justice, out of the loop on the warrantless wiretapping program, and didn’t even share legal opinions about the program with the top lawyers of the National Security Agency that was implementing the intercepts.

But even with this background, I have been astonished at the developments of the last week, with the Air Force and the Library of Congress blocking the Wikileaks web site, and warning their staff not to even peek. I should have known the Air Force would come up with something like this. The Archive's own Freedom of Information Act lawsuit over the last 5 years had already established that the Air Force created probably the worst FOIA processing system in the entire federal government – the federal judge in our case ruled the Air Force had “miserably failed” to meet the law's requirements. But now, apparently, the worst FOIA system has found a mate in the worst open-source information system? This policy is completely self-defeating and foolish. If Air Force personnel do not look at the leaked cables, then they are not doing their job as national security professionals.

Comes now the Library of Congress, built on Thomas Jefferson's books, also blocking access to the Wikileaks site. On the LC blog, a repeated question has been when exactly are you going to cut off the *New York Times* site too? One might also ask, when will you remove Bob Woodward's books from the shelves?

Official reactions like these show how we are suffering from “Wikimania.” Almost all of the proposed cures for Bradley Manning's leak of the diplomatic cables are worse than the disease. The real danger of Wikimania is that we could revert to Cold War notions of secrecy, to the kind of stovepipes and compartments that left us blind before 9/11, to mounting prosecutions under the Espionage Act that just waste taxpayers' money and ultimately get dropped, and to censorship pressure on Internet providers that emulates the Chinese model of state control rather than the First Amendment. So perhaps a first order of business should be to dissect some of what I call the “Wikimyths.”

1. A document dump.

So far there has been no dump of the diplomatic cables. As of yesterday, there were fewer than 2,000 cables posted on the Web in the Wikileaks and media sites combined, and another 100 or so uploaded each day, not the 251,000 that apparently exist in the overall database as downloaded by Bradley Manning. And even that set of a quarter-million cables represents only a fraction of the total flow of cable traffic to and from the State

Department, simply the ones that State staff considered “reporting and other informational messages deemed appropriate for release to the US government interagency community” (the Foreign Affairs Manual explanation of the SIPDIS tag). According to the editors of *Le Monde* and *The Guardian*, Wikileaks is following the lead of the media organizations on which documents to post, when to do so, and what to redact from the cables in terms of source identities that might put someone at risk. Such behavior is the opposite of a dump. At the same time, an “insurance” file presumably containing the entire database in encrypted form is in the hands of thousands, and Wikileaks founder Julian Assange has threatened to send out the decrypt key, if and when his back is against the wall. So a dump could yet happen of the cables, and the prior record is mixed. A dump did begin of the Iraq and Afghan war logs, but once reporters pointed out the danger to local cooperators from being named in the logs, Wikileaks halted the dump and withheld some 15,000 items out of 91,000 Afghan records.

2. An epidemic of leaks.

While the quantity of documents seems huge (hundreds of thousands including the Iraq and Afghan materials), from everything we know to date, all four tranches of Wikileaks publicity this year have come from a single leaker, the Army private Bradley Manning, who is now behind bars. First, in April, was the helicopter video of the 2007 shooting of the Reuters cameramen. Then came the Iraq and Afghan war logs (highly granular situation reports for the most part) in July and October. Now we see the diplomatic cables from the SIPRNet. Between 500,000 and 600,000 U.S. military and diplomatic personnel were cleared for SIPRNet access, so a security official looking for a glass half full would point out that a human-designed security system with half a million potential error points ended up only with one.

A better contrast would be to compare the proposals for dramatic expansion of the Espionage Act into arresting foreigners, to the simple operational security change that the Defense Department has already implemented. The latter would have prevented Manning from doing his solo downloads onto CD, and we should ask which approach would be more likely to deter future Mannings. State Department officials were gloating last week that no embassy personnel could pull a Manning because State’s version of the SIPRNet wouldn’t allow downloads onto walk-away media like thumb drives or CDs. Defense’s rejoinder was that its wide range of forward

operating bases, equipment crashes from dust storms and incoming fire, and often tenuous Internet connections – certainly compared to the usually cushy conditions inside embassies – meant some download capacity was essential. Now, just as nuclear missile launch requires two operators’ keys, and the handling of sensitive communications intelligence manuals requires “two person integrity,” and the Mormons send their missionaries out in pairs, a SIPRNet download would take two to tango.

3. A diplomatic meltdown.

Headline writers loved this phrase, aided and abetted by official statements like Secretary of State Hillary Clinton’s characterization of the cables’ release as an “attack on America” “sabotaging peaceful relations between nations.” In contrast, the Secretary of Defense Robert Gates played down the heat, in a much more realistic assessment that bears repeating. Gates told reporters two weeks ago, “I’ve heard the impact of these releases on our foreign policy described as a meltdown, as a game-changer and so on. I think these descriptions are fairly significantly overwrought.... Is this embarrassing? Yes. Is it awkward? Yes. Consequences for U.S. foreign policy? I think fairly modest.” Most international affairs scholars are calling the cables fascinating and useful, but at least so far nothing in the diplomatic cables compares to the impact on public policy in 2004 from the leak of the Abu Ghraib photographs, or other recent leaks of the existence of the secret prisons, or the torture memos, or the fact of warrantless wiretapping, or even the Pentagon Papers’ contribution to the end of the Vietnam war.

4. Alternatively, no news here.

Wikileaks critics who were not bemoaning a global diplomatic meltdown often went to the opposite extreme, that is to say there was nothing really new in the Bradley Manning cables. The past two weeks’ worth of front-page headlines in the leading newspapers and broadcasts around the world should lay this myth to rest. Folks with more news judgment than we have in this room are continuing to assign stories from the cables, and foreign media in particular are getting an education perhaps more valuable for their understanding of their own countries than of the U.S. Likewise, the blogs are full of lists of stories showing all the things we didn’t know before the cables emerged. The real problem with the modern news media is evident from the fact that there are many more reporters clustered around the British

jail holding Assange, than there are reporters in newsrooms actually reading the substance of the documents. Celebrity over substance every time.

5. Wikiterrorists.

I wish all terrorist groups would write the local U.S. ambassador a few days before they are launching anything – the way Julian Assange wrote Ambassador Louis Susman in London on November 26 – to ask for suggestions on how to make sure nobody gets hurt. I can certainly understand the State Department’s hostile response and refusal to engage with Assange in the kind of dialogue U.S. government officials routinely have with mainstream media, and were already having with the *New York Times* over these particular cables. Given Wikileaks’s prior stance, who in State could possibly have taken at face value the phrase in the November 26 letter which says “Wikileaks will respect the confidentiality of the advice provided by the United States Government” about risk to individuals.

But I wish all terrorist groups would partner up with *Le Monde* and *El Pais* and *Der Spiegel* and *The Guardian*, and *The New York Times*, and take the guidance of those professional journalists on what bombs go off and when and with what regulators. Even to make the comparison tells the story – Wikileaks is not acting as an anarchist group, even remotely as terrorists, but as a part of the media, as publishers of information, and even more than that – the evidence so far shows them trying to rise to the standards of professional journalism.

I was quoted in Sunday’s *New York Times* as saying “I’m watching Wikileaks grow up” as they embrace the mainstream media which “they used to treat as a cuss word.” So far, with only a few mistakes to date, the treatment of the cables by the media and by Wikileaks has been very responsible, incorporating governmental feedback on potential damage, redacting names of sources, and even withholding whole documents at the government’s request. Of course, Assange and his colleagues could revert to more adolescent behavior, since there is the threat out there of the encrypted “insurance” file that would be dropped like a pinata if the organization reaches dire straits. But even then, even if all the cables went online, most of us would condemn the recklessness of such an action, but the fundamental media and publisher function Wikileaks is serving would not change.

6. When the government says it's classified, our job as citizens is to salute.

Actually our job as citizens is to ask questions. I have mentioned that experts believe 50% to 90% of our national security secrets could be public with little or no damage to real security. A few years back, when Rep. Christopher Shays (R-CT) asked Secretary of Defense Donald Rumsfeld's deputy for counterintelligence and security how much government information was overclassified, her answer was 50%. After the 9/11 Commission reviewed the government's most sensitive records about Osama bin Laden and Al-Qaeda, the co-chair of that commission, former Governor of New Jersey Tom Kean, commented that "three-quarters of what I read that was classified shouldn't have been" – a 75% judgment. President Reagan's National Security Council secretary Rodney McDaniel estimated in 1991 that only 10% of classification was for "legitimate protection of secrets" – so 90% unwarranted. Another data point comes from the Interagency Security Classification Appeals Panel, over the past 15 years, has overruled agency secrecy claims in whole or in part in some 65% of its cases.

When two of the CIA's top officers retired and went into business, the *Washington Post's* Dana Hedgpeth asked them what was most surprising about being in the private sector. Cofer Black and Robert Richer responded that "much of the information they once considered top secret is publicly available. The trick, Richer said, is knowing where to look. 'In a classified area, there's an assumption that if it is open, it can't be as good as if you stole it,' Richer said. 'I'm seeing that at least 80 percent of what we stole was open.'" ("Blackwater's Owner Has Spies for Hire," by Dana Hedgpeth, *Washington Post*, November 3, 2007). And this was before the Bradley Manning leaks.

In the National Security Archive's collections, we have dozens of examples of documents that are classified and unclassified at the same time, sometimes with different versions from different agencies or different reviewers, all because the secrecy is so subjective and overdone. My own favorite example is a piece of White House e-mail from the Reagan years when top officials were debating how best to help out Saddam Hussein against the Iranians. The first version that came back from our Freedom of Information lawsuit had large chunks of the middle section blacked out on national security grounds, classified at the secret level as doing serious

damage to our national security if released. But the second version, only a week or so later, had almost no black in the middle, but censored much of the top and the bottom sections as secret. Slide the two versions together and you could read practically the entire document. The punch line is: This was the same reviewer both times, just with almost completely contradictory notions of what needed to stay secret.

The *Associated Press* reported last week (December 9, 2010) that reporter Matt Apuzzo's review of the Bradley Manning cables "unmasked another closely guarded fact: Much of what the government says is classified isn't much of a secret at all. Sometimes, classified documents contained little more than summaries of press reports. Political banter was treated as confidential government intelligence. Information that's available to anyone with an Internet connection was ordered held under wraps for years." The first example AP cited was a cable from the U.S. Embassy in Ottawa briefing President Obama in early 2009 for an upcoming trip to Canada, a cable which "included this sensitive bit of information, marked confidential: 'No matter which political party forms the Canadian government during your Administration, Canada will remain one of our staunchest and most like-minded of allies, our largest trading and energy partner, and our most reliable neighbor and friend.' The document could not be made public until 2019, for national security reasons," the AP reported.

Among other issues raised by the AP reporting is the fact that more than half of the Bradley Manning cables are themselves unclassified to begin with. Why did these items need to be buried inside a system that went up to the secret level? Why couldn't those unclassified cables go up on the State Department's own public Web site? Are they really all press summaries and administrivia? Do they need any further review such as for privacy or law enforcement issues? What objection would the government have to preempting Wikileaks by posting these – that somehow it would be rewarding illicit behavior?

Bringing the reality of overclassification to the subject of leaks, Harvard law professor Jack Goldsmith, who served President George W. Bush as head of the controversial Office of Legal Counsel at the Justice Department, has written, "A root cause of the perception of illegitimacy inside the government that led to leaking (and then to occasional irresponsible reporting) is, ironically, excessive government secrecy." Goldsmith went on, in what was otherwise a highly critical review of the *New York Times*'

coverage of wiretapping during the George W. Bush years (“Secrecy and Safety,” by Jack Goldsmith, *The New Republic*, August 13, 2008), to point out, “The secrecy of the Bush administration was genuinely excessive, and so it was self-defeating. One lesson of the last seven years is that the way for the government to keep important secrets is not to draw the normal circle of secrecy tighter. Instead the government should be as open as possible....”

Goldsmith’s analysis draws on the famous dicta of Justice Potter Stewart in the Pentagon Papers case: “When everything is classified, then nothing is classified, and the system becomes one to be disregarded by the cynical or the careless, and to be manipulated by those intent on self-protection or self-promotion.” In fact, Stewart observed, “the hallmark of a truly effective internal security system would be the maximum possible disclosure” since “secrecy can best be preserved only when credibility is truly maintained.”

Between Goldsmith and Stewart, then, Mr. Chairman, we have a pretty good guide with which to assess any of the proposals that may come before you in the guise of dealing with Wikileaks in these next months. We have to ask, will the proposal draw the circle of secrecy tighter, or move us towards maximum possible disclosure? We have to recognize that right now, we have low fences around vast prairies of government secrets, when what we need are high fences around small graveyards of the real secrets. We need to clear out our backlog of historic secrets that should long since have appeared on the public shelves, and slow the creation of new secrets. And those voices who argue for a crackdown on leakers and publishers need to face the reality that their approach is fundamentally self-defeating because it will increase government secrecy, reduce our security, and actually encourage more leaks from the continued legitimacy crisis of the classification system.

Thank you for your consideration of these views, and I look forward to your questions.

Mr. CONYERS. Thank you so much.

Ralph Nader is well-known, a leading advocate, an author, a lawyer, a Presidential candidate. But Atlantic Monthly has named him one of the 100 most influential Americans in history, and I thought I would put that in the record so that more people than read the Atlantic Monthly would know about it.

We welcome you once again to the Judiciary Committee, Ralph Nader.

**TESTIMONY OF RALPH NADER,
LEGAL ADVOCATE AND AUTHOR**

Mr. NADER. Thank you, Mr. Chairman, Congressman Gohmert, and the other Members of the Committee for this important and timely hearing. A lot of interesting good points have just been made, and there is no point for redundancy.

I would like to mention that we ought to look at the issue of government secrecy and government openness with historic cost benefit evaluation. I worked with Congressman John Moss in 1966 on the first Freedom of Information Act, and I saw the fervent opposition of the bureaucrats in the executive branch to what was then a rather modest piece of legislation. I then worked with him on strengthening 1974 Freedom of Information amendments which made our Freedom of Information Act arguably the best in the world, and I also saw the same opposition. I think that people like Daniel Patrick Moynihan in his book on government secrecy point out that one of the first victims of government secrecy is the Congress itself.

The Congress repeatedly has been repudiated from getting the information in order to perform its constitutional responsibilities such as its warmaking power, its oversight subpoena power, its appropriations deliberations, and many others. Bruce Fein has decried this deprivation of information by the executive branch, vis-a-vis Congress, as a principal cause of weakening what is supposed to be the most powerful branch of our government.

If you look at the historical record, the benefits of disclosure vastly outweigh the risks that come from disclosure. Wars could have been prevented if the American people knew what was going on in the Spanish American war, in World War II, in the Tonkin Gulf resolution, if the American people knew what was going on before the invasion of Iraq with the lies, the cover ups, the distortions that now have been historically documented by the Bush administration, including Richard Clarke, the antiterrorism counselor to President Bush, among many.

What is fascinating about this WikiLeaks controversy is that we have to avoid it becoming a vast distraction, focusing on these so-called leaks instead of focusing on the abysmal lack of security safeguards by the executive branch of the U.S. Government and making those who set up this porous system or who allowed it to be penetrated accountable.

The distraction also is away from the lack of account for executive branch officials who suppress information. How many times have you seen those people prosecuted at the highest levels and the middle levels of government? The suppression of information has led to far more loss of life, jeopardization of American security, and

all the other consequences that are now being attributed to WikiLeaks and Julian Assange.

A million Iraqis have died as a result of the invasion, 5,000 U.S. soldiers, 100,000 sick and injured and traumatized, a country blown apart, more violent opponents to our country, more national insecurity.

We have to be very careful here that the Congress does not stampede itself by executive branch pressure to repeat the PATRIOT Act debacle when this Committee issued a pretty sound piece of legislation with hearings, bipartisan, and then was stampeded along with the rest of the Congress by Karl Rove and George W. Bush with this notorious PATRIOT Act. Stampeded legislation always comes back to haunt its authors.

Furthermore, I am very disturbed by the reaction of Attorney General Holder. I think he is reacting to political pressure, and he is starting to fix the law to meet the enforcement policy, and that is very dangerous. He said the other day, "The national security of the United States has been put at risk, the lives of the people who work for the American people have been put at risk, the American people themselves have been put at risk by these actions that I believe arrogant, misguided, and ultimately not helpful in any way." Referring to the WikiLeaks disclosures via the New York Times and the Guardian and other newspapers.

Those very words could apply to the Bush administration and the Obama administration's military and foreign policy, that they would put us in greater risk. And it is very important for us, especially represented by Congress, that the penchant for secrecy is not nourished further by the WikiLeaks events which are going to unfold in greater magnitude in the coming weeks to leave millions of citizens in our country with a debilitating dictatorial vulnerability to further concentration of authoritarian power in the executive branch.

Floyd Abrams, not known as a radical, arguably the leading First Amendment practitioner in the country, said, in responding to Senator Lieberman's precipitous urging for Holder to indict Assange, he said, "I'd say the potential risks outweigh the benefits of prosecution. I think the instinct to prosecute is rational, and I don't mean to criticize the government for giving it serious consideration, but at the end of the day I think it could do more harm to the national security properly understood than letting it go."

Jefferson and Madison had it right. Information is the currency of democracy, freedom of speech is inviolable, and I would add that secrecy is the cancer, the destroyer of democracy.

We have overwhelming examples, some of which were in your statement, Mr. Chairman, of what happens when information paid for by the taxpayer, reflective of the public's right to know, is kept secret. If you take all of the present and probable future disclosures under the WikiLeaks initiative, the vast majority should never have been classified, the vast majority are reprehensible use of people employing taxpayer dollars, the vast majority should have been disclosed, if not never stated, for the benefit of the American people to hold their government accountable.

Forbes magazine in a cover story in its edition December 20th outlines in an interview with Julian Assange that early next year

the beginning of the disclosure of corporate documents will start. Early next year, Forbes said, "A major American bank will suddenly find itself turned inside out. Tens of thousands of its internal documents will be exposed on WikiLeaks.org with no polite request for executives' response or other forewarnings."

Now the importance of that is the danger of the following coalition appearing in the coming months. You have the government bureaucrats who transcend political parties, the government bureaucrats and the corporate executives who want to destroy the provision for whistleblower protection in the new Financial Reform Act as we speak, that they band together in order to focus on the WikiLeaks and try to stampede Congress and perhaps public opinion into enacting legislation that will further stifle the right of the American people to know and further enhance those who believe that the few can decide for the many and that concentrated power in the executive branch can make a mockery out of the constitutional authority repositied in the U.S. Congress.

We hear a lot about the information age, and we hear a lot about what it is supposed to do for us. But the risk in this WikiLeaks' overreaction to control of the Internet and to damaging a dissemination of compilation and access to information worldwide is very, very serious. That is only one of the consequences that can occur if the Congress allows itself to overreact and if the press does not take a measured view and hold to account those who are calling for executive assassinations, for repressions, for the detonation of due process against people who have received information from internal government sources.

I think the proper range of government security is now being deliberated in the executive branch, but it needs to be stimulated by Congress.

At DARPA, Peter Zatko and his group is busily working on a technical fix so that this kind of disclosure never happens again. Many people think that that cannot be done, that the genie of the Internet is out of the bottle.

But it does seem to me that we should be very careful in conclusion in not developing a bill of attainder mind-set, if I may use that metaphor. If it is okay for Obama administration officials to conspire or collude with Bob Woodward, to use a non-normative intonation of those words, and leak cables and all kinds of secret information and do it with impunity with a reporter who then puts it in a book, it does seem that we are on our way not for developing equal protection policy but for the kind of discriminating policy that will make our legal system not reliable and subject to the distortions of repeated judicial decisions.

Mr. COBLE. Mr. Chairman, I think——

Mr. NADER. I will leave you with that, Mr. Chairman. Thank you very much.

Mr. COBLE. Well, okay, a moot point.

Mr. CONYERS. Thank you, Ralph Nader; and my deep gratitude to all seven of you. This may, in some ways, be one of the finest discussions the Committee has had in the 111th Congress.

I am going to take my time, instead of directing specific questions, to ask all of you or any of you, now that you have heard each other, that you may have a reflection or while you have been here

in the hearing you thought of something you might like to add to your statement already, to have this opportunity to do so now.

Mr. LOWELL. Mr. Chairman, one thing I would like to respond to briefly is the point that my colleague to the left made.

I understand that we are grappling to try to figure out where the First Amendment applies and who is a journalist and who isn't. And I know many have said WikiLeaks and Assange are not because they, to use the phrase, dump data or they don't perform the function of being selective. I think that is a dangerous slope to be standing on, because it puts in the editorial room individual prosecutors who will make the decision as to who is a journalist and who isn't. And to individual courts all over the place as to what deserves First Amendment protection and what does not. And it doesn't distinguish well between what WikiLeaks has done and when a more traditional media outlet posts a document in toto on its Web site. So it makes for, I believe, a difficulty. And I think it is one that cannot be legislated. It has to be decided in another fashion.

But I do want quickly to point out that it is easy to say in American history the function of gathering information from the government by whatever source and disseminating it through the public is classic journalism.

Mr. CONYERS. Yes, Mr. Wainstein.

Mr. WAINSTEIN. Thank you, Mr. Chairman.

I appreciate Mr. Lowell's point, that whatever you ask anybody, be it a court or a prosecutor, to try to distinguish between one person who is a journalist and another person who isn't a journalist is a dangerous slope to be on. Two responses to that.

One is, we are on that slope right now. That is what the law allows as it stands; and Mr. Lowell made that point very well, that the current law allows the government to prosecute both the recipient of the information as well as the leaker of the information.

The second point, though, is if you assume that there is ever going to be a case where a reporter or a person in the position of the news, the recipient of the information, can be charged, then that line has to be drawn.

So go back to the Chicago Tribune cause, which is sort of the classic. 1942, the Tribune actually reports that we have broken Japanese code. If the Japanese had paid attention to it, millions of lives, including many of our parents, might have been lost. They didn't fortunately, and they ended up not prosecuting the case.

But I think many of us or most of us agree that that is a case that is so egregious that that newspaper or that reporter should or could be charged. If you assume that there is such a case and somewhere a line has to be drawn, my point would be is WikiLeaks, aside from whether you want to call them a newspaper or a news organization or not, is their mission and their mode of conduct sufficiently divergent from a traditional news organization, the type that the First Amendment was designed to protect, that it falls beyond that line? So that it could be prosecuted without the First Amendment standing in the way of its prosecution and without other news organizations living in fear—the news organizations that pursue the traditional purpose of news and pursue the traditional modes of conduct of news gatherers and reporters—not live

in fear that, because WikiLeaks got prosecuted, they are going to be prosecuted and, therefore, their actions wouldn't be chilled. That is the argument.

While I agree with Mr. Lowell that any definitional distinction is difficult and can be dangerous, it is where we are right now; and I think WikiLeaks—an argument can be made that WikiLeaks is exceptional enough a situation that a line could be drawn without such damage to the First Amendment.

Mr. SCHOENFELD. Mr. Chairman, I would also compare this case to the Pentagon papers case where the Times spent a great deal of effort redacting the documents before it published them, which is not what is taking place here. This is a very different kind of enterprise. And, of course, in that case, that was a prior restraint case; and the Supreme Court ruled that it was not—the standard had not been met for suppressing that information.

It is also notable that five of the nine Justices said that if the case came to them after publication, as a prosecution they would strongly consider punishing the Times, prosecuting the Times, upholding the conviction of the Times if the information was of the character that was prescribed. So I think that a prosecution of WikiLeaks, just judging by the very scant law we have here, the Pentagon papers case, is a viable possibility.

Mr. CONYERS. Yes, Professor Stone.

Mr. STONE. Thank you, Mr. Chairman.

On the discussion about whether WikiLeaks is part of the press or whatever, I think that is not a fruitless line of inquiry. I agree with Mr. Lowell that drawing a line along those directions is simply not going to be coherent.

But, also, in terms of summary of things, I want to come back to how clear it is from this discussion that the starting point is the classification system, that the bottom line is there cannot be any coherent solution to these issues without going back and examining the classification process and standards. Unless we do refocus what has happened—because, essentially, over the last 70, 80, 90 years, we have run amok with secrecy; and that has created the problems that we have seen here. It has denied the Congress access to critical information, it has denied the courts access to critical information, and it has denied American people access to critical information. Unless and until we go back and fix that, all of this is spinning wheels. I think that is really the place where this Committee and where Congress has to start its inquiry.

Mr. CONYERS. Professor Blanton and then Ralph Nader.

Mr. BLANTON. Mr. Chairman, I just wanted to, at my own peril, try to correct Mr. Schoenfeld's analysis of what is going on here. Because, in fact, a great deal of redaction is going on here on a daily basis. We have extensive descriptions of it in the editors' notes by all the media outlets who are publishing stories on this matter, and they have testified to the fact that WikiLeaks is following their lead after their reporters engage in exactly that discussion with the government about what the risk is, which is a discussion the Chicago Tribune did not have in its case and was its own, I think, journalistic failure, I would argue. So a great deal of redaction is taking place.

And I would just point, also, to a certain trajectory; and I suspect that Mr. Assange's lawyers have maybe read some of Mr. Wainstein's testimony maybe in advance of this hearing, because they are doing some very smart things to eliminate exactly the distinctions that you are trying to draw. They are asking the government for feedback on the documents. They are taking care to follow the lead of the media. They are actually doing the publication in concert with major media organizations who have the capacity that they do not have to do reporting. In fact, they are looking more and more like a media organization.

But I will even step back one from that. Because my reading of the First Amendment as a layperson is that it also protects speech—and this goes to Professor Stone's point—not only freedom of the press but speech. And it seems to me that you will run into really difficult problems not only on the media's slippery slope but on speech. It may go to motivation. It may go to this fact of overclassification.

I pointed out in my testimony in the written statement that one of the most striking things about the Wiki cables that are on the record is the fact that so many of the Confidential and Secret ones shouldn't have been classified to begin with. So you are going to be in a real mess, I think, in any kind of prosecution.

I will leave it there.

Mr. CONYERS. Schoenfeld, you are entitled to a brief response.

Mr. SCHOENFELD. Well, I found myself in agreement with many things that Mr. Blanton said in his statement, but one thing I strenuously disagreed with is the notion that WikiLeaks is responsible in what it is done. It may have indeed redacted some of the documents in the most recent disclosures, but we have had the two previous dumps of large numbers of documents, and I would say 2,000 cables referred to in my judgment is a large number of documents. And these were documents that were also about military operations, field reports.

And I remember congressmen have referred to Secretary Gate's remarks, missing the damage that was done by the latest disclosures. If one looks back at what his remarks were this past summer, he said that the lives of American soldiers and of Afghan civilians who have cooperated with our efforts there were placed at risk. Chairman of the Joint Chiefs of Staff, Admiral Mullen, has said that there is blood on the hands of WikiLeaks. I think these views are entitled to a great deal of respect. The notion that WikiLeaks is responsible seems to me unsupportable.

Mr. CONYERS. Ralph Nader?

Mr. NADER. I would like to submit, Mr. Chairman, with your permission, for the record an article, a short article, in the National Journal called, Breaking the Ranks. Ron Paul vigorously defends WikiLeaks, where he asks his colleagues which events cause more deaths, "lying us into war or the release of the WikiLeaks papers."

I would like to also introduce in the record Harvard Law Professor Jack Goldsmith, who came out of the Bush administration, Seven Thoughts on WikiLeaks, including the description of top Obama administration officials' cooperation with Bob Woodward releasing Top Secret programs, code names, documents, meetings, and the like.

I would also like to include this full page ad in the New York Times today by almost 100 Australians entitled WikiLeaks are Not Terrorists. And it is a rather sober and poignant appeal to Australia's ally, the United States, to cool it.

I would also like to include in the record the full article in Forbes magazine on the forthcoming disclosures in the hundreds of thousands of documents of corporate crimes, corporate abuses, corporate coverups that Julian Assange has assured Forbes would be forthcoming.

And just to reduce our ethnocentrism, Mr. Chairman, I would like to note that WikiLeaks is not just a United States' issue, that there are people in Peru, Kenya, Australia, Iceland, Switzerland, and other countries who have benefited from WikiLeaks' disclosures of rampant corruption and injustice in those countries.

Mr. CONYERS. Without objection, your several documents will be accepted into the record.*

We have a record vote, and so we will take a brief recess and then resume the questioning of the Members. Thank you for your patience.

[Recess.]

Mr. CONYERS. The Committee will come to order. Before yielding to Bob Goodlatte, I wanted to have just 2 minutes further for any of you who wanted to add to the discussion we were in mutually in terms of exchanging ideas and views on comments made by other panelists.

Mr. BLANTON. Mr. Chairman, I think we came to complete and total consensus during that point.

Mr. CONYERS. That is right. As my boy says to me, yeah, right, dad.

Mr. BLANTON. Yeah, right. Anybody want to weigh in? I am looking at Ken, because we had the best argument during the break.

Mr. WAINSTEIN. That is right. But we kissed and made up. I will jump in on just one point, which is everybody has talked about the problem of overclassification. And I just wanted to address that. I agree that is the problem. No question about it. I actually applaud the President for his having undertaken an effort to review the classification processes in place and try to get more transparency and reduce the classification of information.

I guess my point would be this, though. That is a problem. And it is a problem in terms of the reality because it chokes off the flow of information that should go out to the public, information that truly isn't sensitive, but also it is a problem of credibility, because the government has less credibility when it says these are our secrets and only some fraction of them really are. But keep in mind that is one issue. And that doesn't completely solve this problem. So while, yes, we need to address that, the question I think that is out there now that has been posed by WikiLeaks is okay, now what do we do about organizations out there whose sole purpose is to try to get secrets? So I think of this like maybe a football team. A defensive coach on a football team is trying hard to—it doesn't defend well against the run. Well, you don't just fix that

*The material referred to was not received by the Committee at the time of the printing of this hearing.

just by going out and getting a good defensive end, you also probably need a good middle linebacker. So if you look at dealing with overclassification as your defensive end, that is fine, that helps partly. But you are also going to need a good linebacker to try to stop the run.

So my point is we also need to deal with—what do we do with these organizations that are kind of new out there on the scene like WikiLeaks that are doing their best to get our secrets and put them out there?

Mr. CONYERS. Nothing like a sports analogy when we are in complex matters. I would like now to turn to our good friend Bob Goodlatte, who is a senior Member of this Committee, and serves with great distinction.

Mr. GOODLATTE. Thank you, Mr. Chairman, and thank you for holding this hearing. I think this is a very important subject, and this panel has been excellent in offering us a number of perspectives about this. I don't know that we will get quite the unity that Mr. Blanton claimed, but I nonetheless think there is probably increasing agreement on what are the problems and what are the limited solutions that we have. I would say, first of all, that the lack of security safeguards for protecting classified material is stunningly poor. And this problem is enhanced by the use of modern technology that spreads it around in places where I am sure many of the people who want something kept secret don't even know who is responsible for keeping the secret for them. And that is clearly the case with one member of the U.S. Army having access to, and apparently turning over, hundreds of thousands of documents.

Secondly, I second those who have called for greater openness. There are without a doubt many, many things that are classified that should not be. And we have a problem I think with out of control expansion of what are being deemed secrets and for reasons that are not legitimate in terms of somebody wanting to do a little CYA instead of actually really protecting the national interests of the United States.

Finally, we want to make sure that we are not suppressing information that should be made public. Nonetheless, it causes great concern to me that any outside organization would be put in the position of being the arbiter of what amongst hundreds of thousands of documents should be deemed secret, and therefore not put up on the Internet, and what should not. They don't have the professional ability to do that. They don't know the far-reaching consequences that this will have on people's lives or on the national interests of this country. Nor do I get the impression that the leaders of this organization indeed care about what are the national interests of the United States. So we have to address this, first and foremost, by figuring out how to safeguard the things that are truly secret and release the things ourselves that we should be making public, should be disclosing.

So, I guess first my question, I will go to Mr. Wainstein first, but please anybody else join in, in terms of talking about how we change the classification process, what can we in the Congress do legislatively? It seems to me this is primarily a function of the executive branch. But it very much concerns me that the executive

branch has abused this power. And we need to change it. But without some standard, some measure of how these things are classified, what would you recommend that the Congress do to reassert our authority and get the classification process brought under control?

Mr. WAINSTEIN. I appreciate the question, sir. I guess as you pointed out, the first thing to keep in mind is classification is within the prerogative of the executive. So the folks in the executive branch, the ones who decide what should be classified and what shouldn't, and it all sort of boils down to the executive's responsibility to protect national security. That doesn't mean, however, that Congress doesn't have a role. In fact, I think we were talking about this on the break, I think if there is a silver lining to this issue coming up now about WikiLeaks, it is that not only might there be some salutary changes to the Espionage Act, and not only does it, I think, heighten people's awareness of this tension between security and openness, but it also I think might heighten people's awareness of the fact that there really is overclassification. And Congress I think can play an important role in emphasizing how important it is to the executive branch that overclassification be gotten under control, especially if the executive branch wants some legislation out of the Congress as it relates to the Espionage Act, let's say.

The President, as I said, one of his first acts, I think it was early on in the spring last year, was to set up this task force and issue an Executive order covering overclassification. So my sense is there is a sincere effort underway. Keep in mind, however, that while there are, I think, the occasional—

Mr. GOODLATTE. Let me interrupt you because I have got a limited amount of time, and several people might want to comment. But if you have specific ideas about things that Congress ought do in this regard, we would welcome them. And I would ask any other member of the panel.

Yes, Mr. Stone.

Mr. STONE. Yeah, I don't accept this notion that this is in the executive branch's prerogative. It seems to me that the way in which the classification—

Mr. GOODLATTE. I agree that it is not, but I am looking for practical ways to solve the problem. I don't want to argue the point. If you have a suggestion for us to take legislatively, or through appropriations, or whatever, that would help us to reassert our authority in this area, we are interested. I would bet that is on a bipartisan basis.

Mr. STONE. I would say for one that legislation that provided, for instance, that no document or information may be classified unless a judgment is made that the harm of disclosure outweighs—that the harm of disclosure outweighs the benefits of disclosure, as a statutory matter, that would then say that no one could be punished for revealing information that is misclassified under that standard would go a long way to clarifying what the classification standards are.

Mr. GOODLATTE. What if there seems to be some willfulness and deliberate intention to misclassify information that should be classified?

Mr. STONE. Make it a crime.

Mr. GOODLATTE. Okay.

Mr. LOWELL. Congressman, I have two practical things if you consider any amendments to the bill.

Mr. GOODLATTE. Yes, sir.

Mr. LOWELL. First, I have already stated, which is to make sure that we distinguish among the various offenses so that the mishandling of properly classified information is included. Therefore, there is a distinguishing between the various forms of conduct. So Congress is basically telling the executive branch you are not going to be able to prosecute people at the same level for the various kinds of offenses. But the second is to do what the case law often says, be clear that there can be a defense given the intent of the potential criminal defendant for raising the fact something was improperly classified in the first instance.

Mr. GOODLATTE. All right. Anyone else? Mr. Nader?

Mr. NADER. Just a couple of suggestions, Congressman. One is years ago I would say the U.S. Government should declassify anything it knows that the Soviets know so that you don't keep it from the American people. And they knew a lot about what the Soviets knew. But it gets to my point that one of the major players in the whole classification issue is the Congress itself. And when the Congress allows itself to be stratified between the intelligence committees getting classified information and no one else in Congress getting it, that is a way the executive branch co-opts the congressional role and increases the arbitrary classification discretion of the executive branch. So that is something to look into.

And the second is that we should look back at what has been disclosed that was classified to educate ourselves to be able to more precisely respond to your question. Because there is just so many things that have been declassified later or leaked that were absurd to being classified. And that is a good tutorial to develop the kind of nuance that your question involves.

Mr. GOODLATTE. Thank you. Mr. Blanton?

Mr. BLANTON. Congress has an extraordinary track record in pushing back against overclassification. The greatest success I would say in the last 15 years has been the Nazi War Crimes Act that pushed out millions of pages of documents that shouldn't have been kept secret all of those years that showed how we had hired and sheltered Nazis in our own country. Congress ordered that, Congress built the interagency working group that ran it. You should apply the same standards that were in that statute to all historical records, anything more than 25 years old, which under the Executive order is supposed to be treated differently. Apply the Nazi process. Put an interagency working group with some oomph behind it and congressional oversight behind it to make it work. You could break loose that huge backlog of those old secrets that is one of the hugest, biggest credibility problems of the current system. You could make a huge difference.

You could empower the Public Interest Declassification Board, that has appointees from the executive and the legislative branch, to not just make recommendations for changing the system, but really even order the release. You could provide new funding for the National Declassification Center, which is out at the National

Archives, just started in May. Real good idea. They hired a career CIA employee to help oversee it, but they are facing backlogs of 400 million pages of stuff that should have been out 30 years ago. They can't even begin to get their arms around it. A little oversight there I think would really help.

And I think finally, to pick up on Ralph Nader's comment, currently the executive branch treats requests for information from Congress, only the Chairs of Committees are treated as constitutional requests for information. If you are a Member, not a Chair, your request for information is treated as if it was a Freedom of Information request. So join the line that I am in. All right? I am sorry, you have got a higher constitutional duty than I do. And you ought to have the right, all Members of Congress ought to be treated the way Chairs of the Committees are treated today.

Mr. GOODLATTE. Mr. Vladeck.

Mr. VLADECK. Just real quickly, I echo everything Mr. Blanton just said. I would just point you to one more example of Congress taking an active role in this area, which is the Atomic Energy Act of 1954. So here we are not talking about historical records, we are talking about I daresay what we would all agree are some of our most important national security secrets. And Congress did not leave it to the Executive, Congress actually provided detailed statutory procedures to be followed, and indeed to be punished in the breach.

Mr. GOODLATTE. Thank you. These are all very good suggestions.

One other point. The allegation has been made, and I again don't know the truth of this, that WikiLeaks is an organization that has not only released the information on the Internet, but that has been engaged in the solicitation, the facilitation, maybe even the payment of—I don't know—pay for information or pay to facilitate the acquisition of the information. But do any of you have any thoughts on whether there is a need to change the law in this area, or is there adequate law right now against what most people would agree would cross the line between reporting and espionage?

Mr. NADER. First of all, there is a lot more we need to know, Congressman—

Mr. GOODLATTE. I agree with that.

Mr. NADER [continuing]. That we don't know. But for example, obviously Amazon, Visa, MasterCard, with their denial of service in recent weeks, of WikiLeaks, was pressured by the U.S. Government. The U.S. Government did not say cut off the New York Times or the Washington Post. And that is a tip of an iceberg—

Mr. GOODLATTE. I appreciate that that is an issue, Mr. Nader, but it doesn't answer my question, which I have already exceeded the time. Does anybody have any comments on the issue of whether or not we need to strengthen our laws regarding the kind of things that were done or alleged to have been done by WikiLeaks to acquire this information or any other information from the government? And I would contrast from what they acquire from a corporation.

Mr. WAINSTEIN. If I may, Mr. Goodlatte, Congressman Goodlatte.

Mr. GOODLATTE. Yes, Mr. Wainstein.

Mr. WAINSTEIN. I don't know whether WikiLeaks did go about trying to procure or pay for the information. But if there was any

complicity between WikiLeaks and the person who actually pulled the information out of the government, then WikiLeaks could be charged as an aider and abettor, or a conspirator of the leaker. Then WikiLeaks would not enjoy whatever additional First Amendment protections they have as a news organization. Rather, they are charged as a conspirator or aider or abettor of the person who was the leaker. That would be an easier case to make because then they would be charged like the leaker and like the four other leak defendants that have been charged by the Obama administration under the Espionage Act in a way that I think is much less problematic to people because they are not going to be charged as a press organization, rather as someone who is complicit with leaking.

Mr. GOODLATTE. That is under current law, correct? Mr. Vladeck.

Mr. VLADECK. I agree with that. All I would add is it may not be as problematic. It would certainly be as unprecedented. The Espionage Act has not previously been used to my knowledge to prosecute someone on an inchoate theory of liability as an aider, abettor, acoconspirator, et cetera. The text of the statute may support it. I do think we would still wade into some of the issues you heard us describe this morning about applying this antiquated statute to this novel theory.

Mr. GOODLATTE. Thank you, Mr. Chairman.

Mr. CONYERS. Thank you very much, Mr. Goodlatte. We now turn to the gentleman from Virginia, Chairman of the Subcommittee on Crime, Bobby Scott.

Mr. SCOTT. Thank you, Mr. Chairman. And thank you for calling this hearing. One of the problems in passing criminal laws is there are a lot of challenges. If we pass a criminal law, we expect it to be challenged on its constitutionality, so it has to be consistent with precedent. And we have the Pentagon Papers, which alerts us to the fact that anything we do in this area is going to be problematic. Also, the law has to be precise. It can't be subjective after the fact, well, in this case I think it is bad enough to prosecute. The conduct to be proscribed has to be precise.

I am inclined to think that what happened in the WikiLeaks situation ought to be illegal, but I think we have a consensus on the panel, if nothing else, that we ought to take our time and get this thing done right. Let me just ask, I am going to start a couple of issues and just ask everybody to kind of respond to them, one of which my colleague from Virginia just talked about, and that is should it matter whether you helped to obtain the information or you got it slipped under the door, you didn't have anything to do with it in terms of your publication? And does it matter if you knew full well that it was classified? And should it make a difference that it should or should not have been classified?

And second, we have heard a lot about the intent to harm or whether it actually harms. That is going to have a real problem with practicality in criminal law. Because whether or not the leak actually harmed, I mean if you did something to sabotage the Iraqi war and we started that debate, there would be a lot of people who would conclude that you did more good than harm, although obviously if you lose that debate you have committed a crime. And whether or not even though it did harm, you didn't intend for it

to harm. Should that be a defense? And the fact that you redacted some of it but didn't redact all of it, should that help you or not? And part of this is from a practicality point of view, you have been arrested for publishing the material and you get an opportunity to debate the Iraqi war before a jury, and if you win the debate you are not guilty? If you lose the debate you are guilty? If you are lucky enough to be in one jurisdiction where they hate the Iraqi war you are in good shape leaking the material. If you get stuck in another jurisdiction you are in deep trouble. Same crime, different jurisdictions.

From just a practicality point of view, can you talk about some of these kind of issues? And I just yield the panel the balance of my time.

Mr. LOWELL. Congressman, let me give you quick answers to four, and hopefully start the discussion back about the experience about these cases. Theoretically, whether or not a media organization or a third-party are protected either by free speech or free press or petitioning the government changes the dynamic when that organization is, as you or others have said, or Mr. Goodlatte has said, complicit in the theft or the leak on the front end. The problem, again, is the slope. Press people cajole, encourage, flatter, talk to people in the government all the time. They are actively engaged in trying to find out that which the government does not want to disclose. They are involved. They are not taking out a National Enquirer check of a thousand dollars and paying for the information. We think that is a clearer line, although under the First Amendment I am not sure it is. But where do you draw the line then when a journalist is doing her or his job very well and is figuring out ways to cajole somebody to say that which they are trying not to?

So theoretically, I think yes, but I think practically no. I think the issue of whether the media or the third-party or the protected entity knows something is classified, well, the present law doesn't make the disclosure of classified information the crime. It makes disclosure of what is called information relating to the national defense a crime. And we are now seeing with classified overclassification that the fact that it is classified may give a presumption that there is a potential danger in its release. But it is the beginning of the conversation not, and I don't think that is going to be a meaningful distinction today. When you redraw this law someday, it may be one, as again Congressman Goodlatte was saying, how can you prevent overclassification by making sure there is a defense, for example, that if something is improperly classified? So therefore, knowledge that it is classified is not really going to be dispositive.

The intent is very difficult. So you are right, there shouldn't ever be a law that says whether or not the outcome was what you intended; that is, I intended to submarine the policy of Iraq, consequently I did what I did and it didn't submarine the policy. Or in retrospect, it was better to do than not do. It has to be at the front end. It has to be intent. Was your intent to.

Now, that is, as you know, the same in every criminal case. Trying to divine a defendant's intent by whatever their direct statements or circumstantial evidence are is going to be the challenge

even in a classification kind of a case. So again, somebody saying to the government, gee, should I redact? Somebody who meets in public, somebody who does things overtly as opposed to somebody who wears a disguise and is dealing in drop boxes in the middle of the park. You can tell the difference between what somebody's intent is by their behavior.

And finally, you raised a really excellent last point—they were all excellent, but this one as a trial lawyer—when you are divining somebody's intent and you are saying I felt like I needed to expose the fact that there were no weapons of mass destruction, that plays differently to a jury in Alexandria, Virginia, than it might in Washington, D.C., than it might in some other place in the country. And that is why, among other reasons, at least the presumption is so many of these cases are brought in the Eastern District of Virginia, or at least the prosecutors believe they have a more sympathetic jury.

Mr. VLADECK. Could I just add briefly? Congressman, you also raised the specter of putting the jury in the position of deciding whether something was rightly classified or not. And I think it is important to keep in mind that if Congress were to add an improper classification defense into any revision of the law, you are still putting an incredibly high burden on the putative defendant who has taken quite a substantial risk if he really thinks that at the end of the day his freedom, whether he is going to go to jail for 25, 30 years, depends on his ability to convince a jury that something was wrongly classified. So I think, you know, that is not a legal argument, but I do think that that puts a pretty heavy thumb on the scale of why that would not open the door to massive leaks by individuals who thought that things were wrongly classified. Those are pretty severe consequences to take such a long shot on.

Mr. SCHOENFELD. Congressman, I would just add to what my colleagues have said. A number of them have suggested we should alter the law to have an intent to injure. And this was one of your points. I think there is reason to believe that would open the floodgates for leakers, that there are many salutary reasons for leaking, but there could be considerable disagreement about what actually is salutary. The current law, which demands you have reason to believe it could injure the United States, seems to capture behavior that we would really like to keep from occurring, keep genuine secrets secret.

Mr. SCOTT. What burden of proof would you have if somebody honestly believed that this was good for the country, although some juries would conclude it is bad for the country? I mean do you have to prove—would the prosecution have to prove beyond a reasonable doubt that he did not believe that what he was doing was the right thing?

Mr. SCHOENFELD. I am not sure of the answer to that.

Mr. STONE. I think it is important here again to distinguish between—

Mr. SCOTT. So are we talking about a good faith exception to leaking?

Mr. STONE. I think it is important to distinguish between the leaker and the publisher. The leaker can be regulated consistent

with the First Amendment much more aggressively. And there I think it is sufficient to say that knowing disclosure of classified information that is properly classified is punishable.

Mr. LOWELL. Congressman, one more thing on your last point. You know, the present statute and the glean by the courts as to the intent requirement to show, as Mr. Schoenfeld pointed out, that you had a belief that it could injure, whether that is good enough, let me tell you why it is not good enough. What does could injure mean? What if you believed there was a 1 percent chance that it could injure and a 99 percent chance that it wouldn't? Where in that slope does somebody become a felon subject to 20 years in jail? And that is difficult, especially difficult in a First Amendment context.

Mr. VLADECK. Congressman, I think the short answer is you don't write one statute, you write three, right, and that you have one statute that is focused at espionage and spying, you have one statute that is focused on leaking, because as my colleague, Professor Stone, points out, you can impose higher burdens, you can hold government employees to a higher standard, and you have a third statute that deals with private citizens with no intent to harm the national security of the United States. Now, that statute I think is the incredibly tricky one to write. But no matter how it is written, I think having those categories separated out would be such a substantial improvement. And recognizing that the burdens should be different in those three cases would be such a positive development as compared to the status quo, that really I think, you know, almost anything would be beneficial.

Mr. STONE. There is great benefit in having a very rigorous and narrow statute to punish the publication of the information. Because that puts pressure on the government to keep the secret in the first place. So they can't punish WikiLeaks because they don't have the requisite intent or they haven't caused the requisite harm. And if they know that and they are serious about the secrecy, they will then take the steps necessary to keep the information secret. In that dynamic, I think it is very important not to make it too easy for the government to try to prosecute the ultimate speaker. Because if they can do that, then they will get lazy and sloppy on the question of secrecy itself.

Mr. CONYERS. Thank you very much, Bobby Scott, for that interesting exchange. I turn now to the distinguished gentleman from Iowa, Steve King.

Mr. KING. Thank you, Mr. Chairman. I do thank the witnesses. This is an outstanding lineup of witnesses here. And I would direct my first question to Mr. Lowell. Caught my attention in speaking about intent. And in this discussion that we have had, this dialogue about intent, I would be curious as to if you had separate intents and maybe three almost simultaneous, identical acts by different entities with different intents, are they still guilty of the same crime?

Mr. LOWELL. To put flesh on the bones, Congressman King, in my brief introductory remarks today I said the statute—I was speaking about section 793 specifically—could apply, again, first to the government employee who had the confidentiality agreement and then said something or did something that she or he should

not have. And then you have the person he is doing it to. It could be a foreign policy wonk, it could be somebody else. And then you could have the reporter who, as I said, overheard the conversation and published an article. And they are all responsible for releasing the exact same information. They may be releasing it in different ways. Ironically, the last hearer is going to disclose it to the most amount of people. The first person in the confidentiality agreement is disclosing it to the least number of people. And yet it is easier to prosecute the first, as Professor Stone and others said it should be, than the last. So with intent let's take that intent against the last three. As to the government employee, he or she knows that based on the confidentiality agreement, and whatever he or she does, that it is not supposed to occur, and there is very few excuses to go outside of channels to do it. If you protect whistleblowers, then putting that aside, the intent requirement is easier to prove.

To the person who is not in the confidentiality agreement and is actively engaged in the exchange, as were the defendants in the so-called AIPAC case, that was very problematic. Because on Monday, White House officials or State Department officials brought them in to discuss foreign policy that they wanted them to know, and then 3 days later somebody at a different level called them on the phone and talked about the same policy that was the subject of their indictment. Their intent, therefore, could have been proved by showing that what was legal on Monday should not be illegal on Wednesday.

And then finally, when you get to the point of the media, that is where all the comments of the intent requirement, depending on their complicity in the original leak, will make a big difference.

So you can take the same act and have three different standards of intent and still survive, I think, under a constitutional scheme.

Mr. KING. Mr. Wainstein, your comments on that?

Mr. WAINSTEIN. Congressman King, I actually agree with the idea of having sort of this tripartite approach Steve Vladeck and Abbe have described. I think narrowing the provision for each of these different categories is going to make a more targeted piece of legislation.

Mr. KING. Then let me take this to the injury to the United States. What does that mean and how can that be proven?

Mr. WAINSTEIN. That is also another sticking point in the whole WikiLeaks situation. I think you have heard a little bit of that here today. The question of, okay, how damaging was it? Maybe back in the first tranche that came out about DOD, the DOD documents about Afghanistan, there were informants' names, et cetera, et cetera, troop movements and the like. A lot of that stuff ended up getting taken out later on. It is obviously a sliding scale. And when you are dealing with the First Amendment, one of the justifications, especially if you are looking to prosecute a news organization, an organization sort of in the shoes of a news outlet, you have to look at whether you are justifying the prosecution and the incursion on their press activities in order to address real harm to the Nation. And that is one of the big issues I am sure the Department is looking at right now, going through all the things that have been released through these WikiLeaks disclosures and seeing what sort of identifiable pieces of damaging information are in there.

Mr. KING. I don't know that I am clear on this, and I turn to Mr. Schoenfeld. Do you believe the Espionage Act should apply to a foreign defendant that is operating outside the United States?

Mr. SCHOENFELD. I think it could and should be applied. And I think that what he has done, what WikiLeaks has done is to certainly endanger, as a number of ranking officials have said, endanger our forces and endanger allied forces, civilians in Afghanistan and Iraq. The idea that the United States has no recourse in the face of this seems to be unacceptable. And I think looking at the law, that says whoever discloses.

Mr. KING. And while you have the microphone, and for the record again I would appreciate it if you could just summarize those five points that you made in the closing part of your opening statement.

Mr. SCHOENFELD. If I might take the liberty of looking at them. More attention to declassification. Attention to giving legitimate whistleblowers viable avenues other than the media to which they can turn. Reestablishing deterrence of leakers in the government so that those who leak have reason to fear that they will be prosecuted. Bringing down the weight of public opinion against leakers certainly, and against those who publish vital secrets, not just ordinary kind of secrets that are the daily fare of our American journalism. And in some extraordinary cases, prosecution of media outlets that publish secrets which endanger the public.

The classic case that has been mentioned here is the Chicago Tribune case. But there are other cases that have approached that line in recent years. The Pentagon Papers case, the documents that Daniel Ellsberg turned over to the New York Times were historical in nature. There was not a single document in that collection that was less than 3 years old. Some of the material that has, say, been published by the New York Times in the last years since 9/11 have been operational, ongoing intelligence programs like the SWIFT monitoring program. That seems to skirt the line. I ride the New York City subways. And so do millions of others. And there are people out there determined to bomb those. And this is a program designed to stop those people that was compromised. I think the seriousness of that, and I think the irresponsibility of journalism in some cases has been extraordinary in this period. Much, much different from the kinds of things that the Times published in 1971.

Mr. KING. Would you care to speculate on their motive for releasing information that is viewed as classified?

Mr. SCHOENFELD. There were two really substantial leaks in that period. The first was the NSA warrantless wiretapping program. And there the Times had an argument that this was a violation of the FISA Act, and they wanted to bring it to a public stage. I think there is a legitimate debate about that. And they believe I think that they performed a public service. When we come to the SWIFT program, they had been warned by ranking officials, Democrats, Republicans, I think Lee Hamilton, one of the cochairmen of the 9/11 Commission, not to publish this material, and they went ahead. And I don't think they have offered a very convincing justification for doing so. One of the reporters, Eric Lichtblau, said that the story was above all else, and this is a quote, an interesting yarn.

Above all else. Now, for stuff of such gravity, I think one can't imagine a more trivial rationale.

Mr. KING. That answer says selling newspapers. Gentlemen, my clock went red a while back. But I appreciate all your testimony, and I yield back.

Mr. CONYERS. I am pleased to recognize the distinguished gentlelady from Houston, Texas, a very active Member of the Committee, Sheila Jackson Lee.

Ms. JACKSON LEE. Mr. Chairman, let me thank you very much. And I don't want to be presumptuous to suggest that this may be the last hearing of this session, because I know that this Committee works into the very long hours into the night or into the session. But let me thank you very much for your astuteness in recognizing the importance of this hearing for those of us who are in a quandary, if you will. I sit on the Homeland Security Committee and have spent many hours in classified meetings in the crypt, if you will, listening to the array of threats against this country, and frankly, around the world. But I may also, or it comes to mind that if you become too restrictive and you have a law that is ineffective in the espionage law, you also impact what can be the modern day, if you will, whistleblowers. And I know that there has been a distinction made with the Pentagon Papers, sort of after the fact reports, as opposed to these documents that are current and in place.

So I would like you gentlemen to help me with the quandary that I am in. To limit information limits the potential effectiveness of government.

But on the other hand, I don't know whether or not we had a hearing, Mr. Chairman, and I am sure we did, and my memory fails me, but I remember distinctly a sitting Vice President blowing the cover of an active duty CIA agent. And it was interesting to hear the response in that instance. This person's cover was blown, and that sitting Vice President just thought that he was completely right, or either didn't admit it or had someone else, unfortunately, be the fall guy for it.

But I think in the Judiciary Committee it is important to really understand the law. There is some dispute. The WikiLeaks owner, leader indicates that they did write the London ambassador and sought to have certain information redacted and no one responded. But there is a November 27 letter from the State Department saying don't release anything.

Abbe, it is good to see you again. Help me with that. Because there was an effort made. I understand the difficulty of the espionage law is knowing that you are disclosing classified information. Does it have any provision for someone who tried to work with the appropriate persons? Because I guess I see a difference of opinion. I tried to work with you, you did not want to work with me. What is the culpability?

I am going to yield to you first. I just want to talk about the law, and how does that relate to that specific action?

Mr. LOWELL. Very good to see you, Congresswoman, again. Let's distinguish where the law is and how it is applied versus to what people are saying could be done to improve it. So where the law is and where it applies, the elements that you are addressing goes to the following issues: When somebody is accused of violating 793

or 798 under the present Espionage Act, if they are a government employee, we have discussed the fact that they don't have the same back and forth ability to show that they did not have a reason to believe that their conduct would injure the United States or benefit an adversary or a foreign country. So in the context that you are asking and one that this Committee is addressing, which for example might be the WikiLeaks case——

Ms. JACKSON LEE. Outside of that sphere.

Mr. LOWELL. Outside of that or the one you raised. So then the question is the back and forth between Julian Assange to date and the other newspapers and the government officials, here is what I have, what would harm? what would you like redacted? goes to something. What it goes to is when the government prosecutes somebody in that position, that person—the government has to prove beyond a reasonable doubt a certain intent. The defendant in that situation will be able to raise that kind of conduct to show that the intent was not one that had in the mind a reason to believe to injure, but was quite the opposite, that he was doing his best, recognizing what he and others would say was his First Amendment duties to do what was right and also showing his intent was a good one.

The problem is that this is subject to a prosecutor deciding I am still going to charge and let a jury decide that the intent was okay, whatever jury instructions a judge will give, and as one of the other Members said, the differences between trying that case in jurisdiction one versus jurisdiction two on something that is just called intent. And I hope that is responsive.

Ms. JACKSON LEE. It is. And I would like Professor Stone to take a stab at that. And Mr. Lowell, and I want to call him Abbe, we worked in the past, mentioned the First Amendment rights. Do you want to give me some sense of where that plays a role?

Mr. STONE. Sure. Again, I think that the government's ability to regulate the activities of its own employees who have signed secrecy agreements is considerable and that that is where the focus should be, on keeping that information secret if it really needs to be kept secret. That once we move into the realm of public discourse, then we should be extremely careful. And the First Amendment demands that we be extremely careful.

Mr. Schoenfeld a number of times has identified the Chicago Tribune incident from World War II, where the Tribune published information that revealed the fact that we were aware of a Japanese secret code and we had been using that as way of advancing our own war aims. And had that information been made available to the Japanese, as it could have been given the fact that it was published, that would have been in fact a situation where there was a clear and imminent danger that posed a grave harm to the United States. We would have lost a pivotal benefit in fighting World War II. And that seems to me the paradigm case for a situation where the knowing disclosure of that sort of information can be subject to criminal prosecution.

But the key to that example is that it happens once a century. Nothing in the WikiLeaks case comes close to that. And it is important to say that is the situation where you can go after publishers or disseminators of information who are not in a special relation-

ship to the government. And that almost never happens. And when it does happen, it merits punishment. But beyond that, we should be focusing our attention on the situation of keeping information secret in the first place, in house, in the government where secrecy is necessary.

Ms. JACKSON LEE. I like that. Mr. Schoenfeld, you have a different perspective, but I think both of us have I think the same goal. As a Member of the Homeland Security Committee, I don't fool around with potential terrorist threats and/or the new climate we live in. But my quandary is if we freeze down on WikiLeaks, we freeze down even on information that may help us in the war against terror. And I think the professor makes a very definitive point. I am embarrassed that the materials were accessible. How do you respond to that idea?

Mr. SCHOENFELD. I agree with Professor Stone that the Chicago Tribune case really is of a different order problem, that there would have been the kind of immediate and irreparable harm that really does not flow from anything that appears in the WikiLeaks documents. But that is not to say that there is not significant harm from that release. I mean I agree with you we are all better informed now than we were 2 weeks ago before those documents appeared about what our government does. There is no question there is a public benefit that flows from that kind of leak. However, there is the damage done from particular documents themselves which we have only really begun to understand. There are so many different kinds of ramifications from these documents.

But what also has happened is a single blow to the ability of the U.S. Government to conduct its diplomacy in secret, which is a critical task for keeping the peace. If our diplomats or foreign diplomats can't speak candidly to American government officials, we are not going to be well informed about what is going on abroad.

Ms. JACKSON LEE. My message then is first of all, I want our diplomats to speak candidly, and I want our government to come into the world with 21st century technology so that a young military personnel, 23 years old, doesn't have the ability to hack into it. They will handle his case, and I don't think we are discussing that right now. But we do have a burden and a responsibility. You are absolutely right. The candidness I think is appropriate. I understand the pundits have indicated that we look good, but we don't know what else is coming. We look good because we were consistent in our cables to our basic policy. That puts a smile on my face. But the point is that if lives were put in jeopardy—and again I go back to a Vice President that blew the cover of a CIA agent. You know, to me that is a direct threat on some individual's life. If lives have been put in jeopardy, we have a different, if you will framework to operate under. But your message to me is that we now have to get more sophisticated in how we do it.

I see my time. Can I just get the last three witnesses to comment? And I think I missed Mr. Wainstein. But I am going to go this way and then you, sir, if I could just—if you could just quickly. The dilemma, there was an inquiry, and I think Mr. Lowell made it clear that someone's intent is in play here. Mr. Vladeck.

Mr. VLADECK. Congresswoman, I think that is right. The only thing I would add, and you mentioned this at the beginning of your

questioning, is if we are going to focus on the person who is doing the leaking, if we are focusing on the government employee, as I think your colloquy with Professor Stone suggested, the other piece of this is whistleblowing.

Ms. JACKSON LEE. Right.

Mr. VLADECK. And whether and to what extent current whistleblowing laws are adequate to provide opportunities to government employees who have come across what they think is wrongdoing to have remedies other than going to their local newspaper. With that in mind, I think it is just worth noting that I believe last Friday—

Ms. JACKSON LEE. Right, the new appointed person.

Mr. VLADECK. S. 372. You know, I am not an expert on Federal whistleblower laws, but I do think that recognizing that that is part of this conversation, and that strengthening Federal whistleblower laws, especially as they apply to the intelligence community, could actually meaningfully advance this conversation as well by reducing the number of occasions where government employees will feel the need or the lack of other remedies when they come across wrongly classified information.

Ms. JACKSON LEE. If you would, please. Thank you.

Mr. BLANTON. Congresswoman, I think that is a very important caveat to what Professor Stone was saying. That the government has a lot more power to regulate the employee than it does to regulate the media. And I would add overclassification, as does Gabriel Schoenfeld, to that. If we can't deal with the overclassification and we can't really protect serious whistleblowing, then I think the government is not on such solid ground on coming down hard on its own employees and regulating them in that more severe way that Professor Stone says is constitutionally valid.

Ms. JACKSON LEE. Mr. Nader? Thank you. Welcome. Thank you for your service to this Nation.

Mr. NADER. Thank you. I think the point you earlier made, that the disclosures by WikiLeaks can actually enhance our national security. The disclosures do damage. They do damage to government violations, to war crimes, to torture, to the kind of policies that inflame and expand the opposition to us by people who never had any enmity to us. And we can all cite Peter Goss and General Casey and others who basically pointed that out, that our presence in these countries, if we are not careful, provides fertile ground for more opposition and more risks to our national security. So in that sense, these leaks build up public opinion and congressional engagement to hold the government's feet to the fire as a government under the rule of law and under constitutional standards in its foreign and military policy.

Ms. JACKSON LEE. The Chairman has been very kind, if you could just finish, and I will finish.

Mr. WAINSTEIN. Thank you very much, Congresswoman. If I could just associate myself with what Steve Vladeck said about the whistleblower laws. They are a relatively new animal over the last few decades, providing protections for people who see something wrong within their agencies and want to disclose it. And not only do we need to make sure we have sufficient laws to protect whistleblowers and prevent retaliation, but also procedures, user-friendly

procedures in those agencies so that if I am in an agency, I see something corrupt or wrong and I want to raise it up, it is easy for me to do so. I don't have to worry about retaliation. That is important, because obviously if you have the law and the procedures in place that make it easy and seamless to do that, then there is no reason that person needs to go to the press. So in addition to looking at the laws, any oversight that looks at the agencies, especially the intelligence community, to ensure that it is easy for people to blow the whistle without fear I think would be useful.

Ms. JACKSON LEE. Thank you, Mr. Chairman. Just to you, Mr. Chairman, this is a bipartisan hearing. And I just simply want to say maybe as we go into the next session, in a bipartisan way we can look at whistleblower, or as you well know, the No Fear Act that needs to be—which has to do with protecting government employees against whistleblower comments. And I hope we will do that.

Thank you very much, Mr. Chairman. I yield back.

Mr. CONYERS. The Chair recognizes the Ranking Member of the Courts Subcommittee of this Committee, the gentleman from North Carolina, Howard Coble.

Mr. COBLE. Thank you, Mr. Chairman. Mr. Chairman, I want to commend the panelists for their durability today. They have hung tough with us. I appreciate that.

Mr. WAINSTEIN, you mentioned the possibility of enacting a provision to prohibit the disclosure of classified information by government employees regardless of the damage to the national security. What are the pros and cons accompanying such a statute? And do we run the risk of inviting more classification than currently exists in an effort to prevent dissemination of, say, unsavory but not necessarily damaging material?

Mr. WAINSTEIN. That is a very good question, sir. And that actually harks back to something that Abbe Lowell mentioned about how back in 2000 there was—that statute was passed, actually, and then the President Clinton vetoed it. And the statute basically said if you are a government employee, you sign that nondisclosure agreement and you disclose classified information, something that says secret, then you are guilty.

The pro is that that is very clean. You don't have to show damage, you don't have to get into this back and forth of whether it was damaging to disclose secrets about the Iraq war or good because the Iraq war needed to be examined more closely. It is just clear. You have a responsibility as a government employee to protect classified information. You willingly and knowingly disclosed it, you are guilty. So that is on the pro side.

The con side, of course, is that, as you pointed out, there is so much information that is classified that it would be chilling to many government employees when they are going to talk to people that, gee, all it takes is one step over the line, and I get into one iota of classified information and I am guilty. You know, if I intentionally disclose that, I can't talk about anything. And so one of the cons is that it will end up that people will be scared to talk to the press, people will be scared to talk to Congress because they are worried they are going to trip over classified information. And you might have people who will be prosecuted for information which

though classified, as you pointed out, really might not be all that sensitive. It just might be either a matter of mistaken overclassification or something which is embarrassing but not really sensitive.

Mr. COBLE. Thank you for that, sir.

Mr. Schoenfeld, is it your belief that the First Amendment confers on journalists an absolute right to publish classified information or government secrets?

Mr. SCHOENFELD. No, it is not. And I think from what I have heard on the panel, there is some agreement with me that under some circumstances journalists can be prosecuted under the espionage statutes. To hark back to the Chicago Tribune case, we have a case where I think the espionage statutes would apply if the story came out that cost the lives of tens of thousands of U.S. servicemen and prolonged the war. And the Supreme Court of course in the Pentagon Papers case, five of the nine justices, as I had noted earlier, did suggest that if a case came to them not as a prior restraint case, but after the fact as an Espionage Act prosecution or a Section 798 prosecution, they would strongly consider upholding a conviction if the material at issue was material that Congress had indeed proscribed under the statutes.

Mr. COBLE. I got you. Thank you, sir.

Professor Stone, we touched on this but let me run it by you again. Does WikiLeaks enjoy the same protections as traditional journalism organizations, A? And in the Internet age, how do we distinguish between traditional media and the new media? And does the law contemplate such distinction?

Mr. STONE. I think realistically, it is impossible to do that. The Supreme Court itself, in interpreting the First Amendment, has always refused to define who the press is. And in any event, the speech clause, as has been noted, is an independent protection. So although that may be frustrating, I think as a practical reality there is no way to distinguish WikiLeaks from the New York Times or from a blogger. They are all part of the freedom of speech that the First Amendment protects. And that doesn't mean that the conduct that they engaged in may not be treated differently depending upon what they actually do. But I think in terms of the nature of the institutions or individuals, as a practical matter that is not going to be a sustainable line of inquiry.

Mr. COBLE. Thank you. Thank you, gentlemen, for being with us today.

I yield back, Mr. Chairman.

Mr. CONYERS. Thank you, Mr. Coble. I now turn to Bill Delahunt, the distinguished gentleman from Massachusetts.

Mr. DELAHUNT. Thank you, Mr. Chairman. And this has been a very informative discussion. And we are talking about legislation and, you know, the problems of drafting appropriate language and the issues of intent, et cetera. But I still go back to what I said initially. Until Congress, and particularly Members of this Committee, address the issue of the classification process, we are operating in the dark. We don't understand the classification process. I wonder if anyone on the panel really does in terms of the steps. Who classifies? I heard some of you use the term "improper classification." Who makes that decision? I have heard the term "author-

ized leaks.” What in the hell is an authorized leak? Is that a leak that, you know, someone in the Administration can do but we can’t? What struck me again, when I chaired the Oversight Committee in Foreign Affairs, was we would get material that was redacted, page after page after page after page. All you knew or all you saw was the number. And then of course the next day you would read in the newspapers. But I guess that was a good leak as opposed to a bad leak.

So I hope—and I would direct this to my colleague from Iowa—I hope with the new Congress that Congress conducts a series of hearings where it demands an explanation of the process itself. Are we going to rely on a bureaucrat, you know, at a lower level to do the redaction? Who does all this?

Help me with the mystery. Can anyone here? Maybe I see you, Abbe, nodding your head. Give it a shot.

Mr. LOWELL. I can’t answer that question as a blanket fashion across all agencies and all parts of the Department of Defense and all places in the world. But I can answer it based on the materials that I have seen on the cases I have litigated. And you are raising a point. So in the AIPAC lobbyist case, by the time we were done and getting ready for trial there was no fewer than, I don’t know, 4,000, 5,000 pieces of paper that were in a classification mode at one level or another. There is an Executive Order which has criteria for why something is classified, very specific categories of the potential harm that the release of that document or information could cause. Like every other thing you have been talking about today, those aren’t microscopic definitions in a mathematical way. They are subjective to begin with. One, for example, talks about interference with the Nation’s foreign policy or foreign relations—or relations with a foreign country. I mean, what interfered?

Mr. DELAHUNT. What does that mean.

Mr. LOWELL. Well, I mean, then the second question is who gets to decide you ask?

Mr. DELAHUNT. That is the key.

Mr. LOWELL. Well, in many agencies what you will find is that it is not just the Secretary or the Deputy or the Assistant Secretary or its equivalent, it is the lowest level of person working on the subject at the end of every day.

Mr. DELAHUNT. But that is my concern, that is my concern. I think that issue is the predicate for addressing the concerns that you as a panel have addressed. You got to begin there. And we really have to do a thorough review, because I can—I would testify in the next Congress that as Chair of that Committee, I saw material that was classified that was, it was absurd that it was classified. It was just building up a backlog of classified information that ought to be, that everyone in this room today would concur ought to be in the public domain.

The concern that I have is not so much about WikiLeaks but what we are not having access to in a democracy. And again, I hope that in the future, it is addressed, whether it is in this Committee or any Committee, maybe a Select Committee is actually needed, and people coming in who actually do the classification, not the secretary, not the head of the agency, but to hear it.

Now, I had occasion working with Congressman Lungren where we had concerns about information that was being disseminated from the FBI. It was very revealing in terms of how it was done. And I am not saying it was, the classification was done in good faith. But it clearly did not, in my judgment, meet any kind of standard in terms of classification. That has got to be reviewed. Mr. Blanton.

Mr. BLANTON. Congressman, you have got a couple of great assets at your disposal for the next session. There is a terrific review board called the public interest declassification board headed by Marty Faga former head of the National Reconnaissance Office. Smart people are looking at exactly these questions of how do you change it on the front end so you don't—because every single classification decision that a lowly bureaucrat makes generates a stream of cost to the taxpayers and to the efficient flow of information that goes on indefinitely until somebody like me asks for that document to get released. That is a terrible way to do business. It should be automatic after a certain sunset on every one of these secrets.

You can call in those public interest declass board folks so they can give you some expertise. There is a wonderful little office called the Information Security Oversight Office. Those are the folks that audit the secrecy system. They are smart. The head of that office is the guy that coined the term WikiMania that I have been using today in my statement. Call them in and give them some more resources. I think they got 29 people to ride herd on this massive overclassified security system. They need to know. But they can guide you through how does the stamp get made.

And the last thing I would ask, Mr. Chairman, we have done about four different postings that support the consensus on the Committee of massive overclassification. Congressman Poe commented on it, and agreed with Congressman Delahunt actually. It seems that they actually agreed on this. This is actually a piece of White House e-mail that is declassified in a process 1 week apart.

And the first time they cut out the middle, blacked it out, and the second time they cut out the top and the bottom. You slide them together and you got the whole thing. And the punch line is it was the same reviewer, a senior reviewer with 25 years experience. I called him up and said what is up with that? He said, oh, there must have been something in the paper about Egypt that week, but Libya this week.

Mr. DELAHUNT. Exactly.

Mr. BLANTON. We got about five or six Web postings of these kind of graphic illustrations of the overclassification problem that will help you get your arms around it, and I hope do something about it.

Mr. DELAHUNT. Who authorizes the leaks, by the way?

Mr. BLANTON. There is that famous quote from James Baker, the former Secretary of State under President George H.W. Bush. He said, you know, the ship of state is a very unusual ship, it is the only one that leaks from the top. And I think Daniel Schorr once commented when David Gergen was brought into the Bush White House, well, you know, Jim Baker was too busy leaking at the high level, they need somebody to leak at the mid level.

Mr. DELAHUNT. Well, you know, what I find ironic, of course, is the umbrage that some will take about some leaks, but I guess it is not their leaks. There are good leaks and bad leaks, I guess is the bottom line. Mr. Nader.

Mr. NADER. Congressman, part of this goes back to the integrity of the civil servant and protecting it and letting civil servants and people who work in the Armed Forces and the executive branch take their conscience to work. And if you look at the civil service oath of office, it is not to the cabinet secretary, it is not to the President, it is to the highest moral standards. And a lot of this idiocy and overclassification comes from the lack of internal self-confidence that they will have some reasonable protection by civil servants who would say this is foolish to do this.

I will just give you one example. Forty years ago, one agency of the government wanted to get from the U.S. Navy the amount of water pollution coming out of naval bases. And the Navy denied the then-agency dealing with water pollution, they denied the disclosure of the volume of sewage going into the ocean on the grounds that the Chinese and the Soviets could use that information in order to determine how many sailors were on the base. That is a level of foolishness that could have been nipped in the bud if we supported our civil servants and basically recognized that this is, overall, a struggle between individual conscience of people up against the organizational machines that we call bureaucracy.

And we always should bring back the civil service oath of office, very short, very compelling, they all have to take it. We should protect them in making sure that it can be implemented in their daily work.

Mr. CONYERS. Thank you very much. Your additional time was granted at the leave of Steve King of Iowa. We now turn to the distinguished gentleman from Arizona, Trent Franks.

Mr. FRANKS. Well, thank you, Mr. Chairman. I appreciate it. I appreciate all of you folks being here. A challenging subject this morning. I think it is obvious to me, perhaps to all of us, that no human being, regardless of their education or training, is really competent to opine or to know the full extent of the actual damage that a leak like WikiLeaks could cause. I mean, I guess you could put a team of experts together to try to assess the future and the potential undetermined damage, and I just think that it would be completely a hopeless endeavor.

So I am convinced, obviously, that Julian Assange cannot possibly be able to project what the potential damage of what he did is all about. That is a significant point. But in light of that obvious truth, I am wondering if it is time perhaps for us to rewrite our statutes to establish some sort of lower burden for the prosecutor when it comes to proving the likelihood that a leak could cause actual damage and the necessary level of intent under the statute itself.

Mr. Schoenfeld, you mention in your testimony that the ill effects of information leaks can sometimes take years to manifest. And you mention Pearl Harbor and the book, *The American Black Chamber* as an example, which I think is a brilliant example, where the book had disclosed certain things that perhaps could

have prevented Pearl Harbor. And I am going to try get you to expand on that a little bit.

And that our government, I understand, actually considered prosecuting the author of that book but felt like the prosecution and the public nature of it might enlighten Japan even more than what the book did. So I am hoping that you can describe what might have seemed to the outside observer to be the unforeseen consequences of the leaks through the book, and if hypothetically, the author of *The American Black Chamber* were to be tried criminally for disclosing intelligence information today what level of mens rea do you think a prosecutor would be able to show in this case? And I mean, I guess purposeful or malicious intent to aiding the bombing of Pearl Harbor would not be one of them. That probably would be too little too strong. But what about perhaps just recklessness? I know it is difficult to show malicious intent, but yet, the devastation that was caused at Pearl Harbor, you know, my last memory of that reading of the numbers on that war is 50 million dead. It was kind of a big deal, the whole war.

And so in light of this, do you think that we should reconsider the mens rea elements of our espionage statutes? And I have given you a complicated question there. Tell us about *Black Chamber*, tell us how it all fits and how you think that we would approach that today.

Mr. SCHOENFELD. Thank you very much, Congressman, for that very interesting question. Herbert R. Yardley was probably America's leading cryptographer in the 1920's. He was put out of his job after Secretary of State Simpson said, gentlemen don't read other gentlemen's mail, fell on hard times in the Depression and wrote a book called *The American Black Chamber*, basically wrote it to make a pile of money. He laid bare on that book the full history of American code-breaking efforts, including our successes in the Washington Naval Conference of 1921 where we broke the Japanese diplomatic codes and were able to outfox them in those negotiations.

When that book came out, it was treated much like Eric Lichtblau regarded his own story in *The Times* as a kind of interesting yarn. Highly entertaining was what an American newspaper said about it. But in Japan it caused an absolute furor about the laxity with which their own government had treated their codes and ciphers. And it led the Japanese government over the course of the 1930's to invest heavily in additional code security, and they developed a purple machine which was nearly unbreakable. And one of the consequences was that it delayed the—it slowed down the pace at which we, our resurrected code breaking effort, could read Japanese cables.

And we were somewhat behind when Pearl Harbor came along and we missed crucial signals that Pearl Harbor was the intended destination of the Japanese attack. Now, if Yardley were to be prosecuted today, it would be not a hard case because the intent provisions of section 798 which govern communications intelligence are very clear. It is one of those unusual provision in American law where the Act itself is the crime without an intent provision, as far as I remember.

And so there might be a constitutional challenge, but the statute itself does not have an intent requirement. As for relaxing the intensity under the Espionage Act, I am overall very cautious about changing this Act anyway. I think Congress should move very slowly. Widening it has real costs; tightening it has other costs, though I don't have an answer. But I think hearings like this with attorneys, and I am not an attorney who worked closely with the Act, is very much in order.

Mr. FRANKS. Thank you, Mr. Chairman, my time is up. But I really want you to know I appreciate the response, and I hope it kind of puts things in perspective here. Sometimes there is no way to possibly anticipate what certain leaks can cause. And in this case, it really caused Japan to completely rewrite, reassess their codes and potentially could have prevented Pearl Harbor. And in the 9/11 world that we live in, it is a relevant consideration. And I thank you, Mr. Chairman.

Mr. CONYERS. Thank you very much, Trent. But Professor Stone wanted to get one comment in about your question.

Mr. STONE. Thank you, Mr. Chairman. I think it is very important not to get fixated on this question of does the speech cause some harm. One of the things the Supreme Court figured out pretty quickly is that almost all speech causes harm, it is not harmless. And so it made a terrible mistake during World War I, which is that it took the position that because criticism of the war would undermine the morale of the American people, it might lead people to refuse to accept induction into the military, that that speech could be punished because it might have a harm. And what they figured out pretty quickly after that is that was a disaster. That you can't prohibit speech that criticizes an ongoing war because it might have harm. Speech does have harm. And the Pentagon Papers case, although the court said it was not likely in imminent grave harm, even Justice Stewart conceded the speech was harmful, certainly we were revealing all sorts of confidential information about the past, that we had double-dealed with respect to some of our allies, that we made alliances that hadn't been publicly disclosed before, that made it more difficult for us to negotiate in the future. If the standard focuses on harm generally, then you have given up the First Amendment.

Mr. CONYERS. Well, thank you very much. And we thank Trent Franks for raising this line of discussion. I turn now to my good friend, the Chairman of the Court Subcommittee, Hank Johnson of Georgia.

Mr. JOHNSON. Thank you, Mr. Chairman, for holding this very important hearing. Thank you panelists for bearing through it. Before I ask a few questions, I would like to respectfully remind my colleagues that the WikiLeaks organization and Mr. Julian Assange are publishers.

Now, if it can be shown that they, in some way, aided and abetted in the perpetration or commission of a crime, or if they were parties to a crime, then they could be subject to prosecution. But the Justice Department has yet to come forward with an indictment. And until and unless an indictment is issued, then—and until there is a trial on an indictment, then Mr. Assange is entitled to a presumption of innocence by law, and his guilt would have to

be proved by—there would have to be proof beyond a reasonable doubt before that cloak of innocence, that presumption of innocence could be removed from it.

So first I would like to just settle this down and let us look at this situation through that lens. We do have constitutional rights, among which is a right to speak freely and a right to publish First Amendment. And I would also like to point out the fact that all of the documents that were made available to WikiLeaks are not all classified. Some are classified. There have been indications from Secretary Robert Gates that these releases thus far have not significantly harmed overall U.S. interests.

And a quote from Secretary Gates is as follows: The fact is governments deal with the United States because it is in their interest, not because they like us, not because they trust us and not because they think we can keep secrets. And so while there is a public furor about the release of the documents and the information contained therein having been disclosed to the public, we must not get carried away in a fervor as to what has actually occurred.

Now, if these leaks, and I assume that they do undermine national security and the ability of American diplomats to do their jobs, and American personnel who actually engage in compromising this classified information, should be prosecuted, and should be prosecuted to the fullest extent of the law. But unless those criminal allegations are proven, let's be careful and let's insist on that presumption of innocence.

Now, The New York Times is also publishing this information and we aren't shutting down their Web site or encouraging an international manhunt for its editors. And we cannot allow whatever outrage that we may have, whether or not it be justified or not, to cloud our judgment about our fundamental right to a freedom of the press.

Now, we have got to acknowledge that more than just the publishing of this material, this is actually a failure of the U.S. to protect its material. After all, it is a private first class who is alleged to have had access to this treasure trove of information and the ability to download it.

Primarily it is our fault that this information was released, and we need to—and if there is a service, or if there is a positive twist on what has occurred, it is that we have been made aware of a softness in our protection of our important information, and therefore we now, because of public disclosure, we are now in a position to correct and make safer and more fail-proof our information. So for that I would have to thank Mr. Assange for that public service.

Now, we certainly should do a better job of protection instead of embarking upon a crusade to harass and even prosecute publishers of information. And I trust that our Justice Department will look very carefully at this case and the chilling effect that a prosecution that is unwarranted could have on our ability to enjoy our First Amendment freedoms in this country.

The Administration has directed Federal agencies to prohibit their employees from accessing WikiLeaks documents on their work computers. It has also been reported that a State Department employee and alumnus of Columbia University School of International and Public Affairs has warned school officials that stu-

dents interested in a diplomatic career should not access the documents, even from their home computers.

If I may ask Mr. Blanton and Mr. Nader, what are your thoughts about this, and censorship-free Internet access has been a priority for us as we have dealt with other countries, particularly China. And we encourage them to open up to have free Internet or freedom of Internet access. And do you see where our current stance could be—could place us in an untenable position as far as just assuming a moral high ground for making those kinds of arguments to those around the world who don't enjoy the same freedom as we do? Mr. Blanton and then Mr. Nader.

Mr. BLANTON. Mr. Congressman, that wonderful example from Columbia University, I think the best answer to that came from a professor there named Gary Sick, who was a career Navy officer and served on the National Security Council staff under Presidents Ford, Carter and Reagan. Professor Sick stood up, I think, in an open meeting at Columbia and said, if there is any student of international affairs who is not reading the WikiLeaks cables, then they should be thrown out of the profession because this is essential information.

The Air Force is doing this. This is silly. The Air Force is essentially restricting its own open source information gathering. The Library of Congress is stopping the WikiLeaks site. This is just silly. It is self-defeating, it is foolish, I am sure it will end, it doesn't get us anywhere.

And there is the larger question you are going to, and I think this is where the slippery slope that Mr. Schoenfeld was talking about, he thought the Act should apply to foreigners. Well, I have to say on our Web site, the National Security Archive, we published the transcripts of Mao Tse-Tung's meetings with Richard Nixon and Henry Kissinger.

That is top secret information in China. That would certainly be subject to their Espionage Act. So they get a right to come prosecute me on that basis? I am sorry, I don't think so. I think we should look at limiting our own laws and trying to move to a different kind of standard about what transparency we can bring about in governments worldwide.

Mr. NADER. Well, I think those recommendations, Congressman, were, first of all, futile, they can't enforce it, chilling, and induces not the best type of conscientious civil servant or foreign service officer that the student should aspire to. The second point on China is very well put. I think Hillary Clinton is not presently recalling her remarks when she, in effect, if anything, lauded the hackers in China for breaking through Chinese government censorship on the Internet.

And as you implied, we can't lecture the world in one direction and then start engaging in kind of a suppressive activity in our country. Hillary Clinton would be a very good witness before this Committee next year to explain not only what she perceives as the freedom of Chinese hackers compared to other hackers, but also how she has, in effect, done what Secretary Gates has done, which is downplayed the importance in terms of the damage and risk of the release of these State Department cables. The more Gates and

Clinton downplay this, it seems the stronger case Julian Assange has for what he has done.

Mr. JOHNSON. Let me ask if anybody sees any benefits that has accrued from this unauthorized disclosure of documents, of confidential documents, some of which are secret.

Mr. SCHOENFELD. Congressman, I think there are unquestionably benefits. But as Professor Stone mentioned a few minutes ago, there is also always harm.

Mr. JOHNSON. And we have talked about the harm. I just want to talk about the benefits.

Mr. SCHOENFELD. No, I take the point. I think there is—you know, it is hard to dispute that having access, having public access to information that wasn't in the public domain and that should have been is always a positive thing. But, you know, to use the old aphorism, "sunshine is the best disinfectant." You know, I don't think the question is whether there is a benefit. I think that seems pretty clear.

Mr. JOHNSON. Anyone else?

Mr. LOWELL. One quick thing is this is a benefit, this is a clear benefit from these events, because it is allowing Congress to sift through, again, a 100-year-old statute to ensure that it is still working the way it should is against all the other values that we have. So in that sense it has sponsored this kind of public discourse, and we are the better for it, I think.

Mr. JOHNSON. Well, we have some amongst us here in Congress who feel that government is the problem, government is, as soon as it starts putting its hand in things, then everything goes haywire. So I don't know how we resolve that basic conflict, although I guess those folks who would say that the government gets in the way are confining their objections to a commercial context and not a security context. But it is still ironic that there would be those who would chip away, and really hack away at our right to free speech, and a free press, while at the same time, wanting to get government to get out of the regulatory business with respect to commercial activities.

So with that, I will yield back. Thank you, Mr. Chairman.

Mr. CONYERS. You are welcome, Chairman Johnson.

Mr. JOHNSON. And would note that not many are around to listen to my comments.

Chairman CONYERS. The Chair is now pleased to recognize Judge Charles Gonzalez of Texas.

Mr. GONZALEZ. Thank you very much, Mr. Chairman. And Mr. Lowell, thank you very much for characterizing the hearing of the United States Congress as something that is been official that hasn't been the most popular statements in reference to what we have been doing, but thank you.

The first question is, whatever we do here does have implications for matters that are really the jurisdiction of other Committees. But very important, and I think you all recognize this, so I would want a yes or no from each of the witnesses, because we are talking about the conduit, we are talking about the recipient of the information that has been provided them.

Would you agree—well, yes or no, is the Amazon cloud server a recipient, is an Internet service provider a recipient? And Dean Stone, just yes or no.

Mr. STONE. Yes, but it is unconstitutional.

Mr. BLANTON. Yes, but what?

Mr. STONE. It is unconstitutional.

Mr. BLANTON. What's unconstitutional?

Mr. STONE. It created its recipient for purposes of criminal liability.

Mr. GONZALEZ. But the conduit, the medium is a recipient.

Mr. STONE. Under literal definition I would say yes, but I would say it is moot because it would be unconstitutional to apply it that way.

Mr. GONZALEZ. Mr. Lowell.

Mr. LOWELL. Yes, they are a recipient. The statute will apply once they redisclose. It is not a crime to receive, it is a crime to retransmit, which they are doing by allowing people onto their site. And like the professor, I think such an application would be a gross overapplication and unconstitutional.

Mr. GONZALEZ. Mr. Wainstein.

Mr. WAINSTEIN. Yes, Congressman, it would be recipient and I guess it could fall within the statute, but it is very unlikely anybody would ever want to prosecute it. And it would have to await—while there is a provision that says if you retain and did not tell or return the information to the government, under some circumstances, an entity could be prosecuted, it is very unlikely that such an entity would be prosecuted, even if it, in turn, distributed beyond the service.

Mr. GONZALEZ. Mr. Schoenfeld.

Mr. SCHOENFELD. Yes, it is a recipient. I agree with Mr. Wainstein that it is very unlikely that any prosecutor would ever tackle it. There are so many other more blatant leaks that have not been prosecuted; that one seems really a stretch.

Mr. GONZALEZ. Mr. Vladeck.

Mr. VLADECK. Yes, I just echo Mr. Wainstein's point, I think the key is the retention provision of the Espionage Act. I think the government would far more quickly prosecute for retention than for publication. And I think that is where you would see the constitutional problems that Mr. Lowell and Professor Stone alluded to.

Mr. GONZALEZ. Come on, Mr. Blanton, disagree.

Mr. BLANTON. Yes, but should never be prosecuted, just never.

Mr. GONZALEZ. Mr. Nader.

Mr. NADER. No, it is a conduit contractor.

Mr. GONZALEZ. See, I am with you, Mr. Nader. It has huge implications, unbelievable implications. Because then I really think you need to prosecute the person that provided the ink for the newspaper, the person that provided the paper for the newspaper. Why aren't we doing that? And you are saying it is unlikely, but crazy things happen, crazy things happen when people are scared, and there is fear out there.

So this question will go to Mr. Lowell, and let's see who else, it is going to be Mr. Vladeck. You all have given us certain suggestions, and I think they are excellent. And it all comes down to what I think have been basic principles all along, and that is intent. So

let's say we tighten up how we classify information, and we find this formula and we find the arbiter, we have got the criteria, it is tightened down; it is legitimately classified, and then someone violates their oath. That is easy. I mean, that person is going to be persecuted, and he should be—or prosecuted and persecuted likely. And that happens. But now we go to that person that receives the information. And you say that, Mr. Lowell, I think you had introduced a clear and precise specific intent requirement—or that is Mr. Vladeck. Mr. Lowell, carefully define espionage, intent to injure the United States.

How do you define specific intent? You can't just say, well, I saw it and anyone who knows that this is—could be injurious to the legitimate interest of the United States, or do you start having something at that point in time that you should assume, a reasonable person should assume these things?

How do—is it just the traditional principles that we always apply? Because I understand. I think you are on to something that you still have to have the intent. But I never had—I don't recall someone acknowledging that they intended to do certain things when their whole defense is that they are not culpable because they never had that intent. So we end up back on the intent question.

Mr. LOWELL. Well, either Congress will end up in the intent or the courts will end up with the intent issue. And when both of them do, they will look to various things that are, as you pointed out, true in every criminal case to see what a person accused intent by a person's statements, the context in which they acted, and the circumstantial evidence. If a government employee sees that their immediate boss is talking to the press about a topic, that person may have a good faith belief of that is okay to talk about even if it includes classified information.

If a recipient is acting in the context of his or her job as a lobbyist or as a member of the press, or even in a free speech context, and hears something and retransmits it because there is nothing that indicates that it is of any particular damage and it is part of the person's job, it goes to that person's intent. If the person sees that they are operating overtly and not covertly, they are not stealing information, they didn't pay for it, they didn't bribe anybody for it, then there is evidence of their intent.

The issues of bad faith and good faith apply in almost every criminal prosecution in a white-collar context. This is no different, it will just be unique as to what will show the good or bad faith.

Mr. GONZALEZ. Mr. Vladeck.

Mr. VLADECK. I don't have anything to add. I think he is exactly right. The only piece I might tack on at the end is whether there would be circumstances where we would also want to include recklessness, where we might allow for prosecution, short of the showing of specific intent if we can show that the defendant acted completely recklessly and without regard for any of the safeguards that are built into the statute. But I otherwise totally agree with Mr. Lowell.

Mr. GONZALEZ. Mr. Chairman, thank you. I do have one last observation, and that is when we all went to law school, we remember in times of war, the law is silent, remember that? The Con-

stitution is not a suicide pact. The problem in today's world is that wars are indefinite, wars are open-ended, wars are not even declared. That is what really is probably one of the greatest problems for us, is what is, I guess, the new normal out here. Thank you very much, and I yield back.

Mr. CONYERS. I want to thank you very much, Judge Gonzalez, for your concluding the questions in this hearing. This hearing has a certain poignancy because it may be our final hearing in the 111th Congress. But we may be coming back next week, Bob, so I can't be conclusive in ensuring you that this will be my last hearing as Chair.

Mr. GOODLATTE. Mr. Chairman, if you come back, I will come back too. And if you will yield, I would like to say that while it is indefinite exactly how much longer we will be able to call you Mr. Chairman in the official capacity, you will always be Mr. Chairman to all of us. You have done a great job as Chairman of this Committee. You have been very fair to the minority, so we look forward to reciprocating next year.

Mr. CONYERS. Thank you so much. And I want to say to these seven gentlemen that have been with us since early this morning, this may be, in fact, for me personally, one of the most important hearings that the Committee has undertaken. And I am already talking with Mr. Goodlatte about the possibility of subsequent hearings on this same subject in the 112th Congress. And so we thank you as sincerely as all of us can and declare these hearings adjourned.

[Whereupon, at 1:48 p.m., the Committee was adjourned.]

