AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

S. HRG. 111–834

THE ESPIONAGE STATUTES: A LOOK BACK AND A LOOK FORWARD

HEARING

BEFORE THE

SUBCOMMITTEE ON TERRORISM
AND HOMELAND SECURITY

OF THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

ONE HUNDRED ELEVENTH CONGRESS

SECOND SESSION

MAY 12, 2010

Serial No. J–111–91

Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PRINTING OFFICE
63–582 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

VerDate Nov 24 2008 14:12 Feb 07, 2011 Jkt 063582 PO 00000 Frm 00001 Fmt 5011 Sfmt 5011 S:\GPO\HEARINGS\63582.TXT SJUD1 PsN: CMORC

PATRICK J. LEAHY, Vermont, *Chairman*

HERB KOHL, Wisconsin
DIANNE FEINSTEIN, California
RUSSELL D. FEINGOLD, Wisconsin
ARLEN SPECTER, Pennsylvania
CHARLES E. SCHUMER, New York
RICHARD J. DURBIN, Illinois
BENJAMIN L. CARDIN, Maryland
SHELDON WHITEHOUSE, Rhode Island
AMY KLOBUCHAR, Minnesota
EDWARD E. KAUFMAN, Delaware
AL FRANKEN, Minnesota

JEFF SESSIONS, Alabama
ORRIN G. HATCH, Utah
CHARLES E. GRASSLEY, Iowa
JON KYL, Arizona
LINDSEY GRAHAM, South Carolina
JOHN CORNYN, Texas
TOM COBURN, Oklahoma

BRUCE A. COHEN, *Chief Counsel and Staff Director*
MATT MINER, *Republican Chief Counsel*

SUBCOMMITTEE ON TERRORISM AND HOMELAND SECURITY

BENJAMIN L. CARDIN, Maryland, *Chairman*

HERB KOHL, Wisconsin
DIANNE FEINSTEIN, California
CHARLES E. SCHUMER, New York
RICHARD J. DURBIN, Illinois
AL FRANKEN, Minnesota
EDWARD E. KAUFMAN, Delaware

JON KYL, Arizona
ORRIN G. HATCH, Utah
JEFF SESSIONS, Alabama
JOHN CORNYN, Texas
TOM COBURN, Oklahoma

BILL VAN HORNE, *Democratic Chief Counsel*
STEPHEN HIGGINS, *Republican Chief Counsel*

VerDate Nov 24 2008 14:12 Feb 07, 2011 Jkt 063582 PO 00000 Frm 00002 Fmt 5904 Sfmt 5904 S:\GPO\HEARINGS\63582.TXT SJUD1 PsN: CMORC

CONTENTS

STATEMENTS OF COMMITTEE MEMBERS

	Page
Cardin, Hon. Benjamin L., a U.S. Senator from the State of Maryland	1
prepared statement	35
Kyl, Hon. Jon, a U.S. Senator from the State of Arizona	2
prepared statement	39

WITNESSES

Smith, Jeffrey H., Partner, Arnold and Porter, Washington, DC	6
Vladeck, Stephen, I., Professor of Law, American University Washington College of Law, Washington, DC	3
Wainstein, Kenneth L., Partner, O'Melveny and Myers, Washington, DC	8

QUESTIONS AND ANSWERS

Responses of Jeffrey H. Smith to questions submitted by Senator Cardin	24
Responses of Stephen I. Vladeck to questions submitted by Senator Cardin	30
Responses of Kenneth L. Wainstein to questions submitted by Senator Cardin	33

SUBMISSIONS FOR THE RECORD

Lowell, Abbe David, Attorney at Law, McDermott Will & Emery, Washington, DC	43
Smith, Jeffrey H., Partner, Arnold and Porter, Washington, DC	48
Vladeck, Stephen, I., Professor of Law, American University Washington College of Law, Washington, DC	61
Wainstein, Kenneth L., Partner, O'Melveny and Myers, Washington, DC	75

VerDate Nov 24 2008 14:12 Feb 07, 2011 Jkt 063582 PO 00000 Frm 00003 Fmt 5904 Sfmt 5904 S:\GPO\HEARINGS\63582.TXT SJUD1 PsN: CMORC

THE ESPIONAGE STATUTES: A LOOK BACK AND A LOOK FORWARD

WEDNESDAY, MAY 12, 2010

U.S. SENATE,
SUBCOMMITTEE ON TERRORISM AND HOMELAND SECURITY,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The Subcommittee met, pursuant to notice, at 11:03 a.m., in room SD–226, Dirksen Senate Office Building, Hon. Benjamin L. Cardin, Chairman of the Subcommittee, presiding.

Present: Senators Cardin and Kyl.

OPENING STATEMENT OF HON. BENJAMIN L. CARDIN, A U.S. SENATOR FROM THE STATE OF MARYLAND

Chairman CARDIN. The Subcommittee will come to order. We apologize for the late start. As you know, there were votes on the floor of the Senate.

I am going to ask unanimous consent that my entire opening statement be put in the record.

[The prepared statement of Chairman Cardin appears as a submission for the record.]

Chairman CARDIN. I also ask unanimous consent that a letter we received from Abbe Lowell, an attorney and a person I have known for a long time in regards to the challenges he faced in representing defendants under espionage law, also be made part of our record.

[The letter appears as a submission for the record.]

Chairman CARDIN. Let me just start by saying that the purpose of this hearing is to establish a record on the espionage laws of our country. They were developed really in 1917 after World War I to deal with traditional spies who desired to help our enemies. And as Senator Kyl and I were talking about, if you look at the statute, you will see "code books," which I am sure people are wondering what that is today.

It was that concern that motivated the Congress in that time to pass laws to protect our country against our enemies, and that statute has now been used to deal with Government officials who leak information and private citizens who get information and share it, but have no desire at all—in fact, they think they are helping our country, not hurting our country. The question is whether these laws are adequate the way that they were drafted, and today we have three witnesses who are really experts in this area.

VerDate Nov 24 2008 14:12 Feb 07, 2011 Jkt 063582 PO 00000 Frm 00005 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\63582.TXT SJUD1 PsN: CMORC

The purpose is not to take immediate action on a specific bill. It is certainly not an effort to try to deal with the "shield law," which has already been acted upon by our Committee. The purpose really is for us to get a better understanding as to how the espionage law works today with today's technology that was not in existence during World War I, and whether we need to look at a different type of a statute to protect our Nation against both spies and those who have sensitive information and unlawfully disclose that information. And I really do thank our three witnesses that are here to share their expertise with the Committee.

With that, I would yield to Senator Kyl.

STATEMENT OF HON. JON KYL, A U.S. SENATOR FROM THE STATE OF ARIZONA

Senator KYL. Thank you very much, and, Mr. Chairman, thank you for holding this hearing on a subject which is very important and undoubtedly needs to be addressed now. We were talking on the way over about the need probably to replace terms like "code books" with "electronic information" and things of that sort; "national defense," maybe changing that to "national security," and things of that sort. And we really appreciate the recommendations in the testimony. Mr. Smith, I read your testimony last night, and you had a lot of good ideas in there about that.

I also, though, want to focus on something else as well. Let me ask unanimous consent to put my statement in the record.

Chairman CARDIN. Without objection.

[The prepared statement of Senator Kyl appears as a submission for the record.]

Senator KYL. I will just raise the question. I will be interested in the witnesses' basically addressing this issue. We have significant whistleblower statutes on the books now to enable people who have legitimate reasons for disclosing classified information to be able to do so in a protected environment. I do not have a lot of sympathy for people who decide on their own to bypass those statutes, and knowing that the release of information or leak of information to a newspaper, let us say, that is published has the identical effect as releasing that information to a foreign spy would have for the purposes of the enemy, believing that it is OK and then not being able to prosecute it. I would like to get your reaction to that.

And with regard to the question of motive, as I recall, the Israeli spy—I have forgotten his first name; Pollard was his last name—had a very good motive. He did not want to hurt the United States at all, but he did want to help his country of Israel. He is serving life in prison because motive in that case did not matter. It was the effect of the leak of the secrets to another government that was the problem.

So everybody recognizes that leaks are a problem. Nobody seems to have a good idea about how to stop it. And I did appreciate, again, Mr. Smith, some of the ideas that you had in your testimony. But I would like to delve into that a little bit more during the hearing.

So, Mr. Chairman, thank you for, again, raising this very, very important subject, and I think it will be beneficial for our colleagues.

Chairman CARDIN. Well, thank you, Senator Kyl. I just want to underscore the points that you raised because I think this is critical to trying to understand the espionage laws. I was reading the material for today's hearing and was fascinated by the court in the *Rosen* case adding a mental state requirement, which I would be interested to see as we develop this hearing as to how the statute has been basically interpreted by the courts over the last 100 years, changing, I think, the original intent of the statute to try to meet current circumstances. But it may not serve all the circumstances that we have to deal with, and you mentioned the whistleblower issues, and that is a good point. Congress passed the whistleblower statute in order to provide a mechanism where a person working for a sensitive agency could come forward in a protected way. Well, if that employee does not use that process, then are these statutes adequate to deal with it? I think the points that you raise are ones I hope that we will address through the three witnesses.

We have Stephen Vladeck, who is a Professor of Law at American University School of Law. Professor Vladeck is a nationally recognized expert on the role of the Federal courts in the war on terrorism, and has authored numerous law review articles on espionage statutes and terrorism-related issues. He has also been part of the team of attorneys who have been litigating important national security issues relating to the use of military tribunals at Guantanamo Bay.

Jeffrey Smith is currently a partner in the D.C. office of Arnold and Porter. He heads the firm's national and homeland security practice. Mr. Smith previously served as General Counsel of the Central Intelligence Agency and currently serves on the CIA Director Leon Panetta's External Advisory Board. Mr. Smith also serves as General Counsel to the Senate Armed Services Committee, and prior to working in the Senate, he was Assistant Legal Adviser in the State Department and as an Army Judge Advocate General officer. As the head of Arnold and Porter's National homeland security practice, Mr. Smith's clients have included individuals and media organizations involved in leak cases.

Finally, Kenneth Wainstein, who is also currently an attorney in private practice and a partner in the D.C. office of O'Melveny and Myers. Mr. Wainstein previously served as the first Assistant Attorney General for National Security during the Bush administration where he was responsible for the supervision of espionage cases, and also formerly served as a United States Attorney for the District of Columbia. Mr. Wainstein also previously served as General Counsel and Chief of Staff to the FBI Director Robert Mueller.

So we will start with Mr. Vladeck, and then we will work our way through the witnesses. Thank you.

STATEMENT OF STEPHEN I. VLADECK, PROFESSOR OF LAW, AMERICAN UNIVERSITY WASHINGTON COLLEGE OF LAW, WASHINGTON, DC

Mr. VLADECK. Thank you, Mr. Chairman and Senator Kyl. It is an honor to testify before the Committee today on such an important but neglected topic.

Mr. Chairman, you mentioned the importance of the Espionage Act and its significance in our fight to avoid espionage and the implications for our National security. And I think we can all agree that this is an important goal that really cuts across aisles, cuts across ideologies, et cetera.

But as significant as the Espionage Act is, and has been, I think it is fair to say it is also marked by profound and frustrating ambiguities and internal inconsistencies. Attempting to distill clear principles from the state of the Federal espionage laws in 1973, two Columbia Law School professors—Hal Edgar and Benno Schmidt--lamented that the longer they looked, the less they 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 four decades since—and, according to some, increasingly less benign.

My written testimony elaborates upon the statutory scheme in a bit more detail. But for present purposes, suffice it to say that, in my view, there are four significant problems with the Espionage Act in its current form.

The first and most systematic defect to which, Mr. Chairman and Senator Kyl, you both already alluded concerns its ambiguous scope, by which I mean whether it applies to anything beyond classic spying. Enacted to punish "espionage," which Black's Law Dictionary defines as "The practice of using spies to collect information about what another government or company is doing or plans to do," the plain text of the Act fails to require a specific intent either to harm the national security of the United States or to benefit a foreign power. Instead, the Act requires only that the defendant know or have "reason to believe" that the wrongfully obtained or disclosed "national defense information" is to be used to the injury of the United States, or to the advantage of any foreign nation.

As a result, the Act could be applied as currently written to prosecute Government employees or private citizens in cases bearing little resemblance to classic espionage. Such cases could include situations in which a Government employee seeks to reveal the details of an unlawful secret program, or to bring to the attention of the relevant Inspector General or oversight officer the existence of information that was wrongfully classified; and cases in which a private citizen comes into the possession of classified information with no desire to harm our National security. In each of these circumstances, an informed citizen would certainly have "reason to believe" that the relevant information, if publicly disclosed, could cause injury to the national security of the United States. That knowledge, though, need not—and often will not—bear any relationship to the defendant's actual motive. And I think we saw this in the *Rosen* case.

Indeed, in his ruling in the *Rosen* case, Judge Ellis specifically said that the language of the statute leaves open the possibility that defendants could be convicted for these acts, despite some salutary motive, which Senator Kyl already mentioned.

Now, I said there were four significant problems with the Espionage Act. Let me briefly describe what I say as the other three key defects, obviously, upon which I would be happy to elaborate.

Related to the ambiguous scope of the Espionage Act is the question of how, if at all, it applies to whistleblowers. For example, the Federal 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 kept secret in the interest of national defense or the conduct of foreign affairs." Similar language appears in most of the other Federal whistleblower protection statutes.

To be sure, the Federal whistleblower statute, the intelligence community whistleblower statute, and the military whistleblower statute all authorize cleared Government personnel in national security cases to receive information from the putative whistleblower. 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" within the meaning of the Espionage Act—and that itself is hardly clear—might still fall within the ambit of Section 793(d), which prohibits the willful retention of national defense information. Superficially, one easy fix to the whistleblower statutes might be amendments that made clear that the individuals to whom disclosures are supposed to made under these statutes are "entitled to receive" such information under the Espionage Act. But Congress might also consider a more general proviso exempting protected disclosures from the Espionage Act altogether.

Another important and related ambiguity with the Espionage Act is whether and to what extent it might apply to the press. As with the whistleblower example I just described, a reporter to whom a Government employee leaks classified information could theoretically be prosecuted merely for retaining that information and could almost certainly be prosecuted for disclosing that information, including by publishing it. And yet it seems clear from the legislative history surrounding the original Espionage Act that Section 793(e) was never meant to apply to the press; indeed, three other provisions of the Espionage Act specifically prohibit publication of national defense information, and another, broader limitation on the retention of national security information by the press was specifically scrapped by Congress in 1917, suggesting that the Act is express in those few places where it specifically targets news gathering.

Finally, the Espionage Act is also silent as to potential defenses to prosecution. Most significantly, every court to consider the issue has rejected the availability of an "improper classification" defense—a claim by the defendant that the information he unlawfully disclosed was, in fact, improperly classified. If true, of course, such a defense would presumably render the underlying disclosure legal. It is entirely understandable, of course, that the Espionage Act nowhere refers to "classification" since the modern classification regime post-dates 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 broad.

Now, although statutory ambiguity is hardly a vice in the abstract, in the specific context of the Espionage Act, these ambiguities have two distinct—and contradictory—effects. Testifying before Congress in 1979, Anthony Lapham, then the General Counsel of the CIA, put it this way: "On the one hand the laws stand idle and are not enforced at least in part because their meaning is so obscure, and on the other hand it is likely that the very obscurity of these laws serves to deter perfectly legitimate expression and debate by persons who must be as unsure of their liabilities as I am unsure of their obligations."

And to whatever extent these problems have always been present, recent developments lend additional urgency to today's endeavor. In addition to the AIPAC case I mentioned earlier, a report released just last week by the Heritage Foundation and the National Association of Criminal Defense Lawyers highlighted the growing concerns among courts and commentators with the problems of vague and potentially overbroad criminal statutes, even in modern criminal laws, let alone antiquated laws like the Espionage Act. Indeed, just last month, the Supreme Court in the crush- video decision reiterated its concern with Congressional statutes that may chill constitutionally protected speech. As Chief Justice Roberts emphasized for an 8–1 majority, the Court "would not uphold an unconstitutional statute merely because the Government promised to use it responsibly."

Although it is not my place to make specific recommendations to this Subcommittee with regard to how the Espionage Act might be updated, it does seem clear that the current state of the law is counterproductive regardless of the specific policy goals one might seek to pursue. At the end of his decision in the *Rosen* case, Judge Ellis specifically suggested that the time was ripe for Congress to revisit the issue, and, Mr. Chairman, I want to thank you and the Committee for taking up his call.

Thank you.

[The prepared statement of Mr. Vladeck appears as a submission for the record.]

Chairman CARDIN. Thank you very much for your testimony.

Mr. Smith.

STATEMENT OF JEFFREY H. SMITH, PARTNER, ARNOLD AND PORTER, WASHINGTON, DC

Mr. SMITH. Mr. Chairman, Senator Kyl, it is a privilege to be here this morning to address this very important subject.

It is often said that the first responsibility of our Government is to provide for the security of our citizens, and doing so means that some information must necessarily be kept secret—from our adversaries and from public disclosure. And the criminal law plays an important role in protecting that information.

There is no real debate over whether real spies, the Aldrich Ameses, the Robert Hanssens, the John Walkers, and the Colonel Abels of this world should be prosecuted. However, more difficult questions are presented as we seek to prosecute those who leak properly classified information to the press. It is these leak cases that present the hardest questions.

Before turning to the leak questions, let me make three modest suggestions that I think could enhance the ability of the Government to prosecute real spies. And Senator Kyl graciously mentioned a couple of these, as did you, Mr. Chairman.

First, the statutes have a long list of documents that include things like signal book—I have no idea what a signal book is and doubt that the Government still has such things. I think one approach would be to replace it with the words "information in whatever form." If that is too vague, perhaps another approach would be to say "electronic media" or "information in electronic form" in the list.

Secondly, the statutes speak of "information relating to the national defense." I am concerned that language is too narrow. It is true, as courts have, as Judge Ellis points out in his August 2006 opinion, interpreted the term broadly to include information dealing with military matters and more generally with matters relating to the foreign policy and intelligence capabilities. But I do think it should be replaced with the term "national security" and adopting a definition similar to that in the Executive order, that is to say, "the national defense or foreign relations." And I suggest this because I have had some experience, particularly when I was at the Department of State, where we had a prosecution where we had, frankly, to strain to find documents that had been given through a real spy to the North Vietnamese Government that related to traditional diplomatic exchanges.

Third, I suggest the term "foreign nation" be changed to "foreign power," similar to that used in FISA, because we are dealing with al Qaeda and Taliban that are not foreign nations.

Let me turn to the issue of those who leak classified information. Every administration in which I have served has suffered from leaks that have been truly harmful. And every administration has struggled to solve the problem, but none has had much success.

The most recent legislative example was the Shelby amendment in 2002—pardon me, initially 2000. It was vetoed by President Clinton who said it would "unnecessarily chill legitimate activities that are the heart of a democracy." And you will recall the Shelby language was limited only to Government employees, not to the press.

But I think President Clinton's veto put his finger on an important issue, and that is the fact that senior Government officials often talk to the press on background, with authorization, and provide information that is, in fact, technically still classified. But they do so anonymously and without taking the formal steps to declassify the information. What often happens is the journalists then will call around, and they will find out other information related to that part that has been disclosed to them that the administration did not want disclosed, but the person who gets the call from the journalist does not know that the backgrounder has occurred, and it can set in motion a tone that suggests to people that the executive branch is not serious about protecting secrets. I do not want to overstate this, but I do think the key to preventing leaks is discipline from the top.

In other words, when an administration puts out sensitive information, even in the controlled fashion, in a legitimate effort to in-

form the public, they can hardly be surprised when, having permitted the press to pull on the first thread, the whole sweater unravels.

The matter came up again in 2002–2001, I beg your pardon. Instead of enacting the Shelby amendment, the Congress directed Mr. Ashcroft, then the Attorney General, to submit a report, which he did in October 2002. I believe those recommendations still stand admirably, and I urge the Committee to take a look at those and to work with the administration to try to implement some of those ideas which were designed to prevent unauthorized disclosures.

Leaks are a real problem, Mr. Chairman, and I think we need to address them. I have made a few specific suggestions, but I do not think it is necessarily a good idea to open the statute to try to make it easier to prosecute the press. I think that has a lot of issues that just may not—the gain may not be worth the candle.

I want to end by quoting one of my most admired law professors. I was in law school when the Pentagon Papers case—when it was learned that Daniel Ellsberg had admitted to being the source to the New York Times. My professor, who had served a long time in Government, said, "I know what we should do; we should give him a medal and then send him to prison." And that captures, I think, the hard choices that need to be made, and so I commend this Subcommittee for beginning to take a serious look at those hard choices.

[The prepared statement of Mr. Smith appears as a submission for the record.]

Chairman CARDIN. Thank you very much for your testimony.

Mr. Wainstein.

STATEMENT OF KENNETH L. WAINSTEIN, PARTNER, O'MELVENY AND MYERS, WASHINGTON, DC

Mr. WAINSTEIN. Thank you, Mr. Chairman and Senator Kyl, for inviting me to testify before you today along with my two co-panelists, both men of tremendous expertise in the area of counterespionage.

Since the attacks of September 11, 2001, I have spent much of my professional career in the national security world, where sensitive sources and methods are really the lifeblood of our National security operations, and I have seen firsthand the important role that sensitive information plays in our National security operations and how those operations can be put in jeopardy whenever that information is compromised. And, unfortunately, the reality is that that information is compromised all too frequently.

For purposes of today's discussion, I will focus on two general types of unauthorized disclosures: first, where a Government official passes sensitive information to a foreign agent for money or for some traitorous reason, which is the traditional espionage scenario; and, secondly, where a Government official leaks secrets to the media, maybe out of some base self-interest or maybe out of a genuine desire to expose official wrongdoing and improve Government operations.

A key element of stopping both types of disclosures is ensuring that in the appropriate cases we investigate and prosecute those responsible. As you know, however, the Department of Justice has

brought a number of strong traditional espionage cases over the years, but it has brought relatively few prosecutions for leaks to the media. That thin track record is not for lack of trying; rather, it is the result of numerous obstacles that stand in the way of building a prosecutable media leak case. Those obstacles include the following:

First, as a touchstone matter, it is just downright difficult to identify the leaker in most cases, given the large universe of people who often are privy to the information that was disclosed.

Secondly, there are limitations in the Department of Justice's internal regulations, limitations that are in place for all the right First Amendment reasons, but they limit the ability to subpoena and get information from the one party who is in the best position to identify the leaker—i.e., the member of the media who received the leak from the Government official.

And, third, even if you can get beyond that challenge and the leaker is identified, the agency whose information is compromised or was compromised by the leak is often reluctant to proceed because of concern that prosecution is just going to result in the disclosure of further sensitive information.

Then, finally, even if the Justice Department succeeds in identifying the suspected leaker and indicting the case, it can expect to face a very vigorous offense with a wide variety of cutting edge legal challenges, the kind of litigation we saw in the *Rosen* and *Weissman* case that ultimately was dismissed.

For all these reasons, leak cases—especially leak cases to the media—are exceptionally challenging, and the question for today is whether any of these obstacles can be addressed by changes to the governing legislation.

While I do not see one sort of legislative silver bullet that will overcome all these obstacles, I do see a few areas of legislative initiative the Committee might want to consider.

First, for example, the Committee might examine whether Government contractors are adequately covered by the espionage statutes. These statutes were passed well before the influx of contractors into the Government's most secret or sensitive operations, and one of the critical statutes, 50 U.S.C. 783, covers Government employees but does not extend to contractors. Congress could consider putting Government contractors and employees on the same footing in that provision.

Congress could also consider a number of amendments to the Classified Information Procedures Act to ensure better protection of classified and sensitive information in our criminal trials. I have listed a number of ideas for such amendments in my written statement, including several that Senator Kyl has proposed. And with the current national discussion about prosecuting more international terrorism cases in our Article III courts, I think now is a good time to consider amending CIPA to enhance our ability to protect sensitive information in our criminal trials.

And then in a more general sense, I think Congress can use this hearing and any ensuing hearings to encourage respect at a fundamental level for our Nation's operational secrets. Congress can send the message that it does not condone the unauthorized release of classified information about our National security operations.

And it can point out that whistleblowing is no longer a sufficient justification for divulging intelligence community secrets to the public or to the press now that the Intelligence Community Whistleblower Protection Act provides a mechanism where a Government employee who wishes to blow the whistle can actually take that information, that sensitive information, in a protected way to the Intelligence Committees up in Congress.

No matter where one stands on the political spectrum or in the current debate about the various national security policy issues of today, we should all recognize that the unchecked leaking of sensitive information can cause grave harm to our National security. Congress plays a very important role in addressing that problem—whether by legislation, by oversight or simply by exhortation—and I applaud the Committee for the initiative it is showing with today's hearing.

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

[The prepared statement of Mr. Wainstein appears as a submission for the record.]

Chairman CARDIN. Well, thank you, sir, and I thank all three of you for your testimony.

Shortly, this Committee will start the confirmation process of a new Justice to the Supreme Court, and I think there will be consensus among all the members of this Committee that we believe that Congress is the entity to make our laws. And when we see the courts modify our statutes, it reflects either action on the courts that we find inappropriate philosophically, or a failure of Congress to deal with current needs, that needs to be addressed. And I think in the espionage world, it is the latter. Congress has not modernized the statute, and we really need to deal with it.

A prosecutor needs to be apolitical. He must look at the statute and say, "Well, look, if the circumstances fit, it is my responsibility to bring the action." So, therefore, Mr. Smith, when you refer to whether a leak is authorized or unauthorized, I am not sure I find that in the criminal statute anywhere. So it does raise a question as to whether the espionage statute in and of itself needs to be focused toward those who are participating in traditional spy activities, and whether the CIPA statute and others need to be strengthened in order to deal with leaks, or whether we can handle both under one statute or not.

Mr. SMITH. The problem is that the term "authorized leaks" has sort of crept into the lexicon because that is what often happens, as we know. And my concern is that it also sets a tone that somehow enables or empowers others to leak. If they see that a very senior official is talking, then they are less constrained not to talk.

In terms of handling it as a criminal matter, whether one could make those kinds of distinctions and rewrite the statute so that you focus on different types of disclosures that have different purposes in mind, I do not know. But it certainly undermines the effectiveness of the statute when this sort of practice occurs. And what happens, of course, is that you sometimes find an administration talking about A through D in a particular subject, and they are perfectly happy to have that out in the press and talked about because they think it is a legitimate issue. But then when somebody

else puts out F through G on that same set of subjects, they get furious, insist that it is a leak, and refer it to the Justice Department for prosecution and investigation.

Now, you almost never find the leaker, but if you did, one could imagine a very difficult set of circumstances that prosecutors would face in trying to prove where the administration had chosen to draw the line between things that they were comfortable being talked about and things they were uncomfortable being talked about.

So the question, I think, goes back to, as you alluded to in your opening remarks, about who—as did Senator Kyl—who decides what harm will result. That is principally a governmental function, and it is a very difficult line to draw.

Chairman CARDIN. Well, I think it just raises the issue of whether we can deal with the espionage statute in isolation. CIPA and the whistleblower and the other related statutes that we have that are aimed at establishing practices that, when you leak information, you are violating those practices.

Mr. SMITH. I completely agree, Mr. Chairman. If I was not clear, they are linked. There are a number of statutes that fit together, and one ought to look at them comprehensively.

Chairman CARDIN. Is there a difference here in regard to those who sign a non-disclosure agreement with the Government and those individuals who do not sign a non- disclosure? Does that present a different hurdle in regard to current espionage laws or related statutes? Anybody care to——

Mr. VLADECK. I will take a shot at it. You know, I think, Mr. Chairman, it would depend, and I think that is part of the problem with the Espionage Act, is the ambiguity in the language. You know, various provisions refer to whether the disclosure was authorized or not, whether the individual was lawfully in possession of the information or not.

I do not actually think it is a legally dispositive distinction, by which I mean I think you could prosecute an individual under the Espionage Act as currently written, whether they had signed a non-disclosure agreement or not. But I do think that that creates yet another ambiguity. And I suspect that the courts today would find, you know, perhaps more trouble in that ambiguity in the context of a Government employee who had not signed such an agreement; whereas, the one who had signed an agreement might be held to have waived whatever protections he might have had.

But I have to say, I think this actually highlights part of the issue here, which is that the statute is written in such general terms at a time before these kinds of agreements would have even been contemplated by Congress, that if that is a distinction that is worth pursuing, I do not think the current text of the statute would support it.

Chairman CARDIN. Well, one of the complexities here is the statute applies to private citizens, it applies to Government employees, it applies to Government contractors. So there is a whole mix of individuals that this one statute applies to.

Mr. VLADECK. Well, if I may, I think Mr. Wainstein already referred to the issue of contractors. The oddity is that separate from Section 783, Section 793(f)(2) refers to reporting to a superior offi-

cer that you have the information and that you are potentially in possession of classified information. That presupposes that you have a superior officer. So even on the question of whether the statute applies to non-governmental employees, I think the answer just depends on how you cut it. And I think there are concerns with applying it so broadly when the language seems to contemplate chains of command that you might not see in the private workplace.

Chairman CARDIN. Do any of you want to comment about the challenges to a prosecutor under the *Garrity* case where, if the information is required to be disclosed by your employer, it can compromise the ability of a prosecutor to bring that case? Is that something we need to deal with?

Mr. WAINSTEIN. Yes, Mr. Chairman, I would be happy to handle that. The concern you are alluding to is a very real concern in criminal prosecutions across the board—whenever you have a Government employee who gets interviewed as part of an investigation into wrongdoing and is told as a condition of your employment you have to submit to this interview, that employee then gives a statement, and that statement then gets factored into an ensuring criminal investigation and prosecution. The problem is that statement was compelled by the Government, and then that can infect the whole prosecution. Because if you have a compelled statement that gets factored into the investigation and the prosecution should not have been using that statement or knowledgeable about the statement because it was compelled against that person's rights, then it can affect the whole prosecution and really undermine it.

There was the *Blackwater* case recently that has gotten a lot of attention where the case got dismissed for fundamentally that reason.

It is an issue in espionage cases, though I think the way it typically plays out is there is a protocol in place where, if an intelligence agency, let us say the CIA, thinks there has been a leak, they make a referral to the Department of Justice, and there are these 11 questions. It is a standard form, and the agency whose information was leaked answers these questions, sends them to the Department, and the Department of Justice then decides whether or not to initiate a criminal investigation. If a criminal investigation is initiated, then typically the agency stands down on its administrative process so as not to cause that problem.

So there is coordination that avoids that problem, but it is not foolproof. Every now and then, for instance, if a subject of an investigation is working in the agency and there is a criminal investigation going on, that person might just come up for his 5-year re-up on his background and have to go in and be polygraphed. If he is being told, "You have to be polygraphed" and is then questioned about "have you ever disclosed confidential information," and that person then admits it, that compelled statement then gets into the investigation and can taint the whole investigation.

It is an issue that we typically are able to work around in espionage cases. I am not sure that it is something that actually -for which there is a legislative fix that I can think of, but it is one of the problems. I could not recite all the obstacles to successful leak investigations, but it is one of the ones we have to deal with.

Chairman CARDIN. All right. Well, thank you. I appreciate that answer.

Senator Kyl.

Senator KYL. Thank you.

Let me just ask a question. I gather all three of you probably know the answer to this. But in either a leak or an espionage case, I gather that the classification under the law of confidential, secret, and top secret, which—for example, I will just read the middle one. Secret is applied to information "the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security." And there is a higher standard for top secret, a lower standard for confidential.

Is the defense able to go behind that classification in effect to say this information really could not reasonably be expected to cause damage or serious damage.

Mr. VLADECK. Senator Kyl, actually I think the case law is pretty clear that the defendant cannot raise that defense. I think there is a Ninth Circuit decision from the 1970s called *United States* v. *Boyle* that specifically deals with that question, where it would sort of defeat a purpose to allow the defendant to attack in court whether a document was properly labeled.

Senator KYL. Do the others of you agree? So then the President, in effect, or his agents have determined that fact by classifying the information at a certain level. Is that correct? Do you all agree with that?

Mr. SMITH. Yes.

Senator KYL. Oaky. Then let me make this observation, and I am just going to quote—I am just going to pick on one of you, Mr. Smith, because you said it, I think, very well: "Those who become real spies should be prosecuted with the full might of the Government. Those who, without authority, leak to the media or others not authorized to have possession of classified information should similarly be prosecuted."

Now, that is what I want to get to here, that second category. I think we all agree that as to the first category the statutes can be modernized, cleaned up. That is something that you could usefully help us do, but it is that second category where we have some issues. And let me just posit two general points here and then ask the three of you to get into it. And in your testimony, each of you in some way or other dealt with these problems. You have got the problem of the official leak, and I think, Mr. Wainstein, you made this point in your opening statement, that there can be a concern arise among the people in the agency if they see a lot of official leaks being done apparently with some kind of authority. What does that do to the rule of law and their expectation of deterrence? To me, it undermines it. It is not good. But there is an easy solution to it. You either have someone authorize the leak who is in the position of authorizing it. Presumably that happened, if the excuse is this was an authorized leak of classified information. Somebody had to make the decision that it was OK in this for specific purposes to do it.

Well, you can either have that and/or you can declassify the information just before the leak occurs so that there is no question about it.

Both of those seem to me to be preferable solutions to not prosecuting because somebody authorized it—or maybe somebody did not authorize it, and it is hard to distinguish. Reaction?

Mr. SMITH. Since I have spent a fair bit of time thinking about this, Senator—and I think I raised it in my statement—the concern—you have put your finger on it precisely. In an ideal world, when—let us take a real case example. The Secretary of State—there is an upcoming ministerial meeting. The Secretary of State decides that the press should be "backgrounded" on what we are going to talk about. It happens daily. The story in the newspaper the next day says, "Officials close to the negotiations say" da, da, da, da, da, but they cannot disclose their names because they spoke on condition of anonymity. That was probably decided at the Secretary of State's morning meeting the day before, cleared with the White House, and they backgrounded the press.

Somebody made a decision, however, as to where that line would be drawn between what would be given to the press and what would not be. They also felt that they did not want to officially acknowledge that, let us say, the Deputy Secretary of State spoke on the record about this. They like the anonymity. It gives them flexibility. It gets out there——

Senator KYL. Anonymity is Okay. No problem there.

Mr. SMITH. But the problem is nobody then formally declassifies that information so that the documents floating around the Government with the talking points and so on are still technically classified.

Senator KYL. Do you think that is good policy? Or would it not, in fact, be a rather simple and, in fact, important way to solve this problem? Nobody should be leaking information. If the Secretary of State decides that it is a good thing to do, then I am all for it being done. But there should be a simple, quick process by which it can be done, either—you say cleared by the White House. Okay, so that no longer is classified information, correct?

Mr. SMITH. Right.

Senator KYL. Or—and I do not know how you can do this. I guess we would have to provide in law. It may still be classified, but there is an exception for certain officials to leak the information.

Mr. SMITH. Well, I certainly would not be in favor of the latter. I think that is unmanageable. But the former, where——

Senator KYL. But that is what is being done today.

Mr. SMITH. You are precisely correct, and nobody really seeks to prosecute those cases because nobody refers them to the Justice Department. What does get referred to the Justice Department is people who then leak around the edges of that and go further than the administration wanted.

Senator KYL. Excuse me for interrupting, but because we do not have a clear procedure, it gets to be a pretty gray area as to whether you are—when you get the follow-up call from the reporter, are you really adding to that and so on? We need to make that line bright so that we do not get into the Valerie Plame series of telephone call assumptions as played out a year or so ago.

Mr. SMITH. I think that is the solution. It may prove very difficult to administer and to make it workable, because one could imagine the Secretary of State not wishing to send around a piece

of paper that said, "Well, I authorize the Deputy Secretary of State to disclose this kind of information." But in the absence of that, it does seem to me that you have these other problems, and if we could have a system that acknowledged that and somehow regularized it, I think it would be valuable for a variety of reasons, including hopefully discouraging others from leaking things that should not be leaked.

Senator KYL. Yes, exactly. Thank you.

Just in the 20 seconds I have left, comments by the other two panelists on that particular point? Then I will make my second one later.

Mr. WAINSTEIN. I am sympathetic to your point, Senator, about the nebulousness of the authority issue, and, you know, I think it is worth pursuing whether there is a brighter line that would be in some ways more easily administrable and maybe even fairer.

Mr. VLADECK. And just quickly, because I suspect we will come back to this, I also think that this conversation presupposes that we are all in the same place with regard to the current regime for classification and that we are willing to accept that the current regime for classification works adequately both in ensuring that the right information is classified and that the wrong information is not. And I guess, Senator, I would just say that is not an assumption I am necessarily comfortable making.

Senator KYL. I appreciate that that is a different question, though, and it is one that deserves examination. But we have to start from a premise and—Okay, good. Thank you very much.

Chairman CARDIN. I want to follow up on Senator Kyl's point because I agree with him, and I want to just go through a couple scenarios. Some of it is personal because we get sensitive and classified information that we read about in the paper, and we are always puzzled as to how much we were restricted.

But let us take that Secretary of State example and the person who is responsible to give the information to the communication person who is making it available on background, mistakenly gives pages 1, 2, 3, when they are only supposed to give pages 1 and 2. All the information is classified.

Where is the legal responsibility there? I guess I do not understand authorized leaks from the point of view of the criminal culpability under the statute. To me, if you intentionally give our information that is sensitive, there is vulnerability. I understand the court is interpreting this with intent to harm our country, and this is certainly not with intent to harm our country. But how do you draw this line if you do not have in practice a procedure that Senator Kyl has talked about where the information is no longer classified as sensitive or classified?

Mr. SMITH. Well, I would defer to Mr. Wainstein on the issue of prosecutions because that is difficult. But it does—you have put your finger on a critical question. I think that in the absence of that kind of a system, I do not know where the criminal culpability should be, but I have seen instances in which a Secretary of State asked an Assistant Secretary of State to background the press, the Assistant Secretary went further than the Secretary wanted, thinking, however, that he was carrying out what the Secretary directed him to do. The Secretary got very, very angry and eventually wrote

a letter to the Assistant Secretary. That was a disciplinary action. And it was a lack of clear communication about exactly what the Secretary wanted disclosed.

Given the time pressure on these officials, it is hardly a surprise that that happens, but this is a criminal statute where clear lines—we need to make an effort to try to draw as clear a line as possible.

Chairman CARDIN. That is my point and I think Senator Kyl's point. There needs to be a process here, because let me take it then to someone who is not on the same page here. Someone—let us take from the Congress of the United States—who has been shared the same information in a classified setting and then sees it released by background without name by the administration. Is that Congressman then permitted to share that information and comment on it? I think the answer is no, but where do you draw the line? It seems to me that if you do not have a process that has some transparency to it on the information that is permitted to be released. It is a very fuzzy situation, probably not too much documentation to back this up, and if you get an aggressive prosecutor—who has independence, remember. Our prosecutors do not have to wait for an invitation to investigate. They can do that on their own. Aren't we going down a path that could be extremely difficult to administer?

Mr. SMITH. It is extremely difficult to administer, and it is often not fair. I have known Members of Congress of both parties to complain that the administration will come up and brief the Congress on some particular project or a program and say this is top secret, you cannot talk about it, and then it leaks that very afternoon. And it leaks in a way that the Members of Congress disagree with because the administration has decided to put out their version of things, and Congress feels constrained from talking to the press and saying, well, we disagree with that, we think it is bad policy. And they are inhibited because of the classification that the administration has put on it. It is not right. I have seen it done—this is truly bipartisan. It is done by both parties in both administrations, and it is not right. And it is certainly not right then to sort of threaten prosecution to somebody, particularly a Member of Congress, who chooses to say something to the press that is counter to what the administration has put out.

So greater transparency is critical. How one does that realistically would be difficult. But you are both correct that it is not right the way it is currently working.

Chairman CARDIN. Well, I think the answer is what Senator Kyl is suggesting. There has to be a transparent process for declassifying that information if it is going to be made available to the public. I mean, the Secretary of State is going to have to say these two pages are just no longer classified and they are available. Therefore, we all know that, and we can comment on it. But to say that it is still classified but the press gets it on background only, preventing the open discussion of it by those who have knowledge of its content is wrong.

Mr. SMITH. There is a countervailing interest, which is the hard part here, which is that it is important for senior administration officials to put information in the public so that the public will

know what is going on and be talking about it. They often do not want to do it in a way that specifically ties officially the administration to that statement. I mean, the FOIA litigation over the years has recognized that as a viable distinction between something that leaks and later an official acknowledgment of the leak, which then does declassify it. So it has its useful part.

But what troubles, has always troubled me about it is that there is—who is the decider here? Who gets to decide what is classified and what is not? And I have seen administration officials try to play it both ways, and then to use the criminal law to try to enforce that seems to me deeply troubling.

Chairman CARDIN. I want to ask one more question, if I might, and that is about the Whistleblower Protection Act, S. 372 in the 111th Congress. I think all three of you are familiar with the operations of the CIA. The whistleblower statute that we have provided—how does that work with the CIA trying to carry out its mission? Is this the right way to provide relief for employees who have concern? Or do you believe it prevents the CIA from—or hampers the CIA in its mission?

Mr. SMITH. The answer is I do not know, Mr. Chairman. I would be happy to think about that and get back to the Committee. In my experience with the agency over the years, it has not been a problem. But I think it is a question, and with your permission, let me think about it a little bit and get back to the Committee.

Chairman CARDIN. I appreciate that.

[The information referred to appears as a submission for the record.]

Mr. WAINSTEIN. I'd like just sort of to talk about the general notion of having a mechanism in place where members of the intelligence community, employees of the intelligence community who see something going wrong that they want to disclose, that they can take it through classified, protected channels and get it to the Intelligence Committees whose job it is to practice oversight and to root out wrongdoing, root out problems.

I think that is exactly the mechanism we need to perfect, and I have not studied the new bill, but to the extent that more work should be done to make sure that that process is in place, it works well, there are user-friendly procedures in place so that whistleblowers can get that information up to the Intelligence Committees through the IG, the CIA IG, up to the Intelligence Committees, and then not be retaliated against for it, I am all in favor of it. And I think it is important because the more we have a workable process in place for that, then the less people can justify their unilateral leaks of classified information on the grounds that they were trying to blow the whistle. And a lot of leaks to the media are that, and they are well intentioned at some level. But at the end of the day, they are unilaterally disclosing sensitive information that can cripple our operations.

Mr. VLADECK. If I may briefly, Mr. Chairman, I would just add to that. I think relying on the whistleblower statutes makes a lot of sense subject to two points. The first is that presupposes that either the general counsel of the CIA or the Intelligence Committees are in a position to act on this information. And there has certainly at least been some suggestions by commentators and critics that

the law actually does not necessarily allow especially the Intelligence Committees to take necessary steps beyond that. I think that is a difficult question.

Secondly, even if we all agree that that is the exact process we want to be followed, the Espionage Act is silent as to its interaction with the Whistleblower Protection Act. And so at the very least, I suspect we might find common cause on the notion that one could specifically amend the Espionage Act to exclude protected disclosures under the various Federal whistleblower statutes so that we do not have the concern of a chilling effect that it might be unclear, even where the whistleblower laws appear to apply, that these disclosures will not subject the relevant individuals to prosecution.

Chairman CARDIN. Thank you.

Senator Kyl.

Senator KYL. Thank you, Mr. Chairman. This is a good example of a hearing that could actually produce something useful as opposed to much of what we do.

Let me get to——

Chairman CARDIN. I think that is a compliment.

Senator KYL. It is very much a compliment.

[Laughter.]

Senator KYL. The second main thing that I wanted to get to, we talked during my first questioning about the so-called official leak, and I think we came to a conclusion that there needs to be a brighter line and a better transparency so that the official leak becomes the authorized official statement of unclassified information somehow.

The second is the sort of good motive leak, either an individual thinking "I know better than the President what the administration's policy ought to be, and I am going to leak some information that undercuts his policy," knowing that it is going to get out in the public—and it was Jonathan Pollard; I remembered his name—or maybe even this AIPAC case. I only know what I have read about it in the newspaper, but it seemed to me that I recall one of the defenses, or at least discussions in the media was that whatever information may or may not have been exchanged there, it was not with an intention of hurting the United States, and that was Pollard's defense.

But it seems to me that that is also dealt with fairly easily by two things, but the statute maybe needs to be amended to guarantee this. Mr. Vladeck, you got close to this, I think, in one comment you made.

First of all, there are two things, it seems to me, that easily respond to the mens rea requirement here. One is the classification itself, if, in fact, the classification is a per se determination of harm if the information gets out; and, second, the mens rea here would consist of two other factors: one, knowing that it is unauthorized and intentionally leaked or put out. In other words, you did not mistakenly pick up the wrong page—I think maybe, Mr. Smith, that was your example. You were supposed to release page 2 and 3 and you mistakenly released page 1 as well. You would have to know that what you released was unauthorized; and, second, you would have to do that intentionally. And the harm requirement would be satisfied by the classification itself.

It seems to me that as to the person who is doing the leaking, a statute that was clear in those respects would satisfy everything that we need except for—and I am leaving aside, at least for the moment, the publication by a media corporation. In other words, we are not talking about here, at least for the purpose of doing this in pieces right now, prosecuting someone for publishing the information. Leave that aside for a moment. I am just talking about the person who leaks the information. Wouldn't that satisfy the statutory requirements, and if we stated it that way, it would be much clearer and much easier, therefore, to prosecute?

Mr. SMITH. Let me take a first cut at that, Senator Kyl. If this statute that you are discussing is focused on the Government employee or the person who had authorized access to the classified information, I agree with you, that is pretty close to what the provision in Title 50 does.

I am uncomfortable with having it be a per se determination that if the President classified it, that is sufficient. I still think the Government should have some requirement to prove that that, in fact, harm could reasonably be expected to occur because I do not—I am a little suspicious of the administration overclassifying things.

Senator KYL. If I could interrupt you, though, I thought you all three agreed that under the case law today, it is not a defense that the information—in other words, the defense does not go behind the classification to determine the reasonable probability of harm.

Mr. SMITH. You are correct. That is what the case law is. But I am a little bit of an outlier on this.

Senator KYL. So you are suggesting that standard may need to be modified in some——

Mr. SMITH. Yes.

Senator KYL. Okay.

Mr. SMITH. But the hard part is then when it is then given to somebody else who does not have authorized access to it and whether the statute that you have just outlined should be applied to them. And, again, I think I am pretty comfortable with it absent the——

Senator KYL. Well, let me just argue with you there 1 second. First of all, you do not want judges who obviously do not have the experience in dealing with classified data that the executive branch that does the classification does. That has been a criticism of giving judges this ultimate determination.

Secondly, if the problem is that information is too easily classified, the individual who is doing the leaking still understands that his leak of that is unauthorized, whether he disagrees with that proposition or not. And it seems to me there are other ways that you deal with that other than just deciding to "take the law into your own hands."

Mr. SMITH. I completely agree with you. My only concern is that I think there does need to be something more to put somebody in jail than simply somebody put a classification stamp on it. I am troubled with that mere fact.

Mr. VLADECK. If I may jump in, I would just add to that, Senator Kyl. I also think it is worth noting that the case law to which both Mr. Smith and I adverted largely pre-dates the enactment of the Classified Information Procedures Act and largely pre-dates the

sort of belief—the creation of a body of case law where Federal judges have, in fact, become expert to degrees that we may disagree about, at least have some experience in handling classified information in criminal trials. And so it is possible that some of the concerns that led to these decisions, at least initially, have been abated at least somewhat by CIPA.

Senator KYL. Mr. Wainstein.

Mr. WAINSTEIN. You will recall that Attorney General Ashcroft was asked to look at this issue, look at—I guess it is called the Shelby bill, which essentially said what it is that you are referring to, Senator, basically said that if you are a Government employee—I think also former Government employee—and you knowingly and intentionally leak classified information, that you committed a crime.

I think the concern about overclassification is not case specific; it is just sort of the broader concern that it puts too much authority in the hands of the President to decide what is classified and, therefore, what can be criminally—when someone can be criminally sanctioned for disclosing it. And it might give the Executive too much leeway to maybe classify information that really is more embarrassing and less actually a matter of national security. That is sort of the broader issue.

And then, of course, there is the question of even if you had a statute like this, would it really help increase the number of prosecutions? In some ways, it would be easier because, I mean, it means that the prosecution would not have to prove up the harm, the potential harm, so you would not have to go into, let us say, talking about how the information that was disclosed was about some operation over in Europe that we were doing and how that was—really that disclosure was harmful because that operation would have given us the following intelligence benefits. Whenever you have to do that in order to make your case, you stand the risk of having to disclose more information in discovery and in the actual presentation at trial.

A statute like this would lower the burden, make it easier to meet the burden, because all you have to show is it is classified. And you would not have the same danger of releasing more classified information. But I think that there are those countervailing concerns about over-classification.

Senator KYL. Do you mind if I just follow up? You say it would lower the burden, but I am still confused. While the—is it *Boyd*? What is the Ninth Circuit case?

Mr. VLADECK. I am sorry. I believe it is *United States* v. *Boyce*?

Senator KYL. Boyce. Well, that case may have pre-dated CIPA. It is at least still acknowledged by the three of you as probably the law in this situation until it is further refined. So would what I am proposing really be a change from the law, at least as it pertains to going behind the classification? In other words, would it be setting up a higher standard?

Mr. WAINSTEIN. It would not be setting up a higher standard. The prosecutor would not have to prove the harm element.

Senator KYL. But does he have to prove that today beyond the classification?

Mr. WAINSTEIN. Yes, the classification helps, but you have to put on additional evidence, typically, and that is what happens. In fact, that is often one of the reasons why a case like this might not be pursued because of the concern that you have to disclose sensitive information in doing that.

Senator KYL. So you have to do that—I am now a little confused. Maybe you can see why.

Mr. VLADECK. Senator Kyl, if I may, and I hope this alleviates the confusion. I think that the differences between whether the information counts as national defense information under the Espionage Act versus whether the mens rea that the Supreme Court has read into the statute in the *Goren* decision that the defendant knew that the information both was national defense information and could harm—knew or had reason to believe that the information, if disclosed, could harm the national security of the United States. So it is not—knowing that it is classified in and of itself may not be enough, especially if any reasonable person would be hard pressed to see how that information, if disclosed, could cause harm.

Senator KYL. So, again, with your permission—and the two of you agree with that reading?

Mr. SMITH. Yes.

Mr. WAINSTEIN. Yes.

Senator KYL. So there is a requirement that the Government, with some degree of burden, prove that the individual knew that national security could be harmed above and beyond the fact that he knew he was leaking classified information.

Mr. VLADECK. That is my understanding of the cases, and I think just to go back to Chairman Cardin's point from before, the Supreme Court, I think, has adopted that construction largely to save what it thought would be constitutional difficulties with the lack of such a requirement, at least in 1941.

Mr. SMITH. And my experience with these cases is the fact that it was classified is used as evidence to establish that it relates to national security—pardon me, relates to national defense and that its disclosure would cause harm. So it is—the first thing that prosecutors do is say, Was this properly classified and why?

Senator KYL. Well, if I could then, just to summarize my view on this, it seems to me, with that clarification—and I really appreciate that—that with that further requirement, it is hard to justify a good-motive leak when, in order to prosecute such a case, you would have to establish that he knew that he was potentially harming the national defense of the United States.

Mr. VLADECK. Senator Kyl, this just goes back to a point I made in my opening statement, and perhaps you and I just disagree on this. I think there is a difference, though, between knowing that the information you are disclosing may potentially harm the United States and having that be the motivation for why you are disclosing it. There might be good faith separate from your knowledge. Perhaps you are not the right person to make that calculation if you are the Government employee, but I would resist the assumption that an employee could never have good faith simply because he knows that the information is classified.

Chairman CARDIN. On that point, Senator Kyl, it seems to me you are all saying, though, that, leaving the publication issue aside, as Senator Kyl has suggested—we really do not want that to be the focus of our work here today. But what you are saying is that you do limit this to Government or former Government employees like the so-called Shelby bill, that it should not apply to private individuals. I am again talking about the *Rosen* case, clearly one that is before us. Do you believe that is a different standard?

Mr. SMITH. In the case of the person who had—the laws and the regulations speak in terms of people who had authorized access. That is either Government employees, former Government employees, or contractors. There I think the Government has been able to prosecute these cases. I think the fact that it was classified, that the individual knew it was classified, and disclosed it without some kind of formal authority, that ought to be prosecuted. In the case of the—the *Rosen* case, you will recall that the man at the Department of Defense named Franklin who gave them the information was prosecuted, and he is in jail for a long time. That I think is proper.

I think what we are talking about is making it easier to prosecute those cases by doing some of the things we are talking about, perhaps working in some of the idea that if it is properly—that if it is classified, that should be sufficient, but the Government would still have to—I think we are all, at least most of us are agreeing that simply the fact that it has got a classification stamp on it should not be sufficient to send somebody to jail for 25 years. I think you need a little bit more than that.

The difficulty comes in when it gets into the hands of somebody who did not have authorized access. If that person then passes it to a foreign government intentionally knowing that the foreign government is interested in it, then I think that, too, should be a crime. If the person to whom it is passed seeks to publish it, either in a newspaper or puts it on Facebook or a blog someplace, then that gets a little bit harder because presumably the person is putting it out there because he or she believes that somehow it is important to talk about. That still, in my mind, is a crime, but the motive and the purpose gets a little bit more complicated there because they may genuinely believe that it is a mistake that this particular issue is not being discussed.

So perhaps we need to have a statute with different types of action, different intents, and different punishments, depending on the actor and the intent.

Mr. VLADECK. And if I may, I come at this from a slightly different perspective, from the sort of academic long view. I think the problem, Mr. Chairman, with going past the individuals who are authorized to have the information is that it becomes very difficult, as Mr. Smith says, to draw the line once you get into the unauthorized access category. You said you wanted to bracket the question on publication. I think that makes sense. But I think that is the elephant in the room here, which is that once we cross the line from those individuals who are legally entitled to receive the information to those who are not as a category, that question comes into the conversation. And so——

Chairman CARDIN. It certainly does, but we are really trying to concentrate here on people who specifically are giving information out to individuals more so than the news media issue.

Mr. VLADECK. And I think that that goes to—I agree with Mr. Smith's suggestion that we might think of—if I take it to be a suggestion, that in those cases we might look at a more rigid intent requirement as compared to the Government employee or the contractor who should simply by virtue of his office know and be required to hold onto this information. The private person we might think about changing the standards because of these concerns.

Chairman CARDIN. Senator Kyl.

Senator KYL. Well, Mr. Chairman, let me just say I have got a lot of other questions. I also have a lot of other meetings because we were so late here. This is an excellent panel. I really hope that we can call upon you as we start to try to formalize how we might want to respond to all of this for your advice in helping us craft ideas for our colleagues perhaps. I really appreciate all three of you informing the Committee. It was a very helpful hearing, and I hope we can count on your free advice in the future here.

Chairman CARDIN. Well, let me just echo what Senator Kyl has said. The purpose of this hearing was for us to gather information, to get better informed, and to start a record in this Committee as to the challenges we have. It clearly will require us to look beyond just the espionage statute itself. CIPA clearly is involved, the whistleblower statutes. It is certainly an issue also concerning not just the passing on of information but publishing. We understand that is an issue that ultimately comes into the equation, but what we were looking at is to try to set up the right formula for the types of activities that compromise our National security. I think as Mr. Smith said, changing the definition is one I think we all would agree needs to be done.

This has been very, very helpful to us. The hearing record will remain open for 1 week for additional questions and statements, and I thank our three witnesses. We stand adjourned.

[Whereupon, at 12:13 p.m., the Subcommittee was adjourned.]

[Questions and answers and submissions for the record follow.]

QUESTIONS AND ANSWERS

Questions for the Record from the Senate Committee on the Judiciary, Subcommittee on Terrorism and Homeland Security Hearing, "The Espionage Statutes: A Look Back and A Look Forward"

Responses from Jeffrey H. Smith

Question (1)
If the espionage statutes were narrowed to only address classic espionage cases, do you have any specific suggestions for legislation that would address the following issues: (a) the unauthorized disclosure/transmittal of classified information by current and former government employees and contractors who do not intend to aid a foreign nation or harm the United States; and (b) the unauthorized disclosure/transmittal of classified information by private persons who are not government employees or contractors who do not intend to aid a foreign nation or harm the United States.

(a) I believe there is merit in narrowing the espionage statutes to create an offense for a current or former government employee or contractor who has or had authorized access to classified information to knowingly convey that information to a person not authorized to receive it. This formulation would, as your question points out, eliminate the requirement in the current law that the government prove that the individual has "reason to believe [the information] could be used to the injury of the United States or to the advantage of any foreign nation." (18 USC 793 (d)).

Under this new statute, the government would have to prove merely that the individual had authorized access to classified information and knowingly gave it to someone not authorized to receive it. The government would still have to prove that the information was properly classified; specifically that its unauthorized disclosure could be expected to cause harm to the national security. As I testified, I believe that the term in current law, "information respecting the national defense", is too narrow. I prefer the term "classified information" and would define it as information properly classified in the interest of national security under the authority of a statute or an executive order by the President.

51680845v1

63582.001

The simplicity of this approach has great appeal, but also raises a number of questions and invites potential criticism. It is similar in some respects to the amendment sponsored by Senator Richard Shelby that was enacted in 2000 but subsequently vetoed by President Clinton. As with the Shelby Amendment, some will see it as an "Official Secrets Act" and will chill the free exchange of ideas, particularly between government officials and the media. They will contend that it also makes criminal the sort of discussions that occur constantly around Washington at think tanks and in academic circles. Finally, they will argue that it sharply limits the ability of former government officials to write books or teach as they will be unsure whether the issues and facts they discuss are - in some corner of the government - regarded as classified.

These concerns are real, but the government also has an interest in putting some teeth in the statutes that are designed to protect properly classified information. Leaks to the press have caused real damage and the Shelby Amendment was intended to make it easier to prosecute government employees who "leaked" to the press.

After the amendment was vetoed, Congress sought the views of the Attorney General on the challenges presented by unauthorized leaks of classified information and the adequacy of current law. Attorney General Ashcroft, in a letter dated October 15, 2002, replied that:

> I conclude that current statutes provide a legal basis to prosecute those who engage in unauthorized disclosures, if they can be identified. It may be that carefully drafted legislation specifically tailored to unauthorized disclosures of classified information generally, rather than to espionage, could enhance our investigative efforts. The extent to which such a provision would yield any practical additional benefits to the government in terms of improving our ability to identify those who engage in unauthorized disclosures of classified information or deterring such activity is unclear, however.

I appreciate Attorney General Ashcroft's reasoning. In fact, I am not aware of an instance in which the Justice Department was unable to investigate or prosecute a government employee because of the language in 18 USC 793 requiring proof that the individual had reason

51680845v1

to believe that the information could be used to the injury of the United States. However, over the last few years there have been some developments that I believe argue in favor of narrowing the statute to eliminate the knowledge requirement in the case of unauthorized disclosures by government employees or contractors.

The major change that has occurred is the effort to shift the approach that intelligence and law enforcement agencies from "need to know" to "need to share". This shift aries, of course, from the failure of the agencies to adequately share information about the 9/11 hijackers that might have prevented the attacks. As part of this process, the "wall" that had slowly been erected as a result of judicial rulings and policy choices between the law enforcement and intelligence agencies was breached - by changes to the Foreign Intelligence Surveillance Act and by policy changes. Although much progress has been made in the sharing of information, the recent failure to prevent, Umar Farouk Abdulmutallab, the "Christmas bomber", from getting on a plane bound for the United States with a bomb concealed in his underwear has increased pressure for additional sharing of intelligence information among agencies. This is a laudatory goal but also results in many more individuals having access to much more highly classified information than in the past. And, this information is in digital form that can be moved easily by electronic means - as appears to have been the case in the Wiki leaks case - or transported out of government facilities in tiny devices.

This greater access to information by many more individuals increases, it seems to me, the need to have a statute that makes it easier for the government to investigate and where necessary prosecute individuals who have authorized access to classified information and disclose it without authority. Hopefully such an approach would also serve as a deterrent to those contemplating a leak.

51680845v1

63582.003

It might even help with so-called "authorized leaks". These "authorized leaks" take a number of forms, but are most often a conversation "on background" or "off the record" between a senior executive branch official and a reporter. In my experience, most of these conversations are "authorized" by even more senior officials or are conducted by an individual, perhaps a cabinet secretary, who has original classification authority (and hence also has declassification authority). The purpose of these conversations is often laudatory, that is a senior person in the executive branch makes a determination that the information should be made public, but not as an official statement by the government. A typical case is a trial balloon of positions that the President will be taking at an upcoming summit meeting. This informs the American public about the US policy and stakes out a position to which other heads of state must react - hopefully making it more difficult for them to reject the American position. A related question is, however, if the information was made available to the public through an "authorized leak", how can the government continue to maintain that documents containing the same information are still properly classified?

Other "authorized leaks" are, however, less helpful. Many such leaks occur when there is a policy dispute within the administration and senior officials speak to the press about positions they believe the President should adopt. They may do so in an effort to influence public opinion in favor of their position or to discredit the position of those in other departments with whom they disagree. They may be sufficiently senior that they have the technical authority to declassify the information, but in taking on themselves the decision to do so without getting specific authority or technically declassifying the information and making it public, they risk violating the law. At a minimum, such selective leaking of classified information undermines the credibility of the system.

51680845v1

On the other hand, our democracy places great faith in free and open debate. Therefore, the prosecution of a government official who leaks merely to influence a decision or disclose improper activity should be undertaken only after very careful consideration by the Department of Justice. One could imagine for example, that the Attorney General would authorize prosecution only when the leak did, in fact, result in harm to the nation. In cases of lesser harm or when there were other countervailing circumstances, the matter could be dealt with by administrative actions by the individual's agency. These may include loss of clearance or even termination from government employment.

Finally, let me encourage the Subcommittee to follow up on the other suggestions in Attorney General Ashcroft's letter that are designed to reduce the number of unauthorized disclosures. My experience is that leadership from the top, increased internal discipline and a reduction in the amount of information that is classified are key measures that must be taken to prevent - or at least reduce - unauthorized disclosures of classified information.

(b) Prosecuting individuals who are private citizens without authorized access to classified information for transmission of classified information to unauthorized persons is a difficult question. I do not think it prudent to modify current law so that such persons may not be prosecuted if they did not intend to harm the United States or to benefit a foreign power. In general, I think the current laws are adequate and permit prosecution of those who, in my judgment, ought to be prosecuted. We should remember that other governments have used the press and "research institutes" for intelligence purposes. For example, during the Cold War TASS, the official Soviet News Agency, operated largely under the control of the KGB. We should anticipate that hostile governments or terrorist groups will use similar tactics in future and

51680845v1

63582.005

I think we should leave the laws as they are in order to make prosecution of such activity possible.

Question (2)

During the Subcommittee hearing, questions were asked which focused on the relationship between the whistleblower protection statutes and the espionage statutes. Do you have any views on the Intelligence Community Whistleblower Protection Act, Title VII, §§ 701-702, Pub. L. 105-272, and S. 372, The Whistleblower Protection Enhancement Act of 2009, which has been favorably reported by the Senate Homeland Security and Government Affairs Committee, in regard to the following issues: (a) whether either of these statutes will hamper CIA or other intelligence agency operations; and (b) whether the statutes contain sufficiently user friendly procedures for intelligence community employees.

(a) and (b) I have not had any direct experience with the Intelligence Community Whistleblower Protection Act and therefore my response is based on reviewing the statute, the hearings on S. 372 and my general experience in the Intelligence Community over many years. In brief, I support the concept of whistleblower protection in order to encourage federal employees to report instances of waste, fraud or abuse to Congress. In the Intelligence Community, getting the procedures right is especially important, not only to protect properly classified information but also to give employees an outlet so they are not tempted to leak to the media. I believe the success of this program can only be determined by analyzing the number of times the procedures established in the Act have been used. I believe it would also be instructive to determine how many employees in the Intelligence Community are even aware of the existence of this law.

To answer your questions directly, I am not aware of any instance in which these statutes have hampered the functioning of the CIA or the broader Intelligence Community. Furthermore, although the procedures are complex, I do not believe that if they were used in good faith by employees and the agencies they would hamper the functioning of the Community.

51680845v1

AMERICAN UNIVERSITY
WASHINGTON, DC

STEPHEN I. VLADECK
Professor of Law

June 3, 2010

The Honorable Patrick Leahy
Chairman
United States Senate Committee on the Judiciary
Washington, DC 20510-6275

Dear Chairman Leahy:

At your request, this letter contains my responses to questions offered by members of the Subcommittee on Terrorism and Homeland Security arising out of my testimony at its May 12 hearing on "The Espionage Statutes: A Look Back and a Look Forward." I would ask that these responses be included within the formal Committee record of the hearing.

In particular, Senator Cardin asked me to address two questions:

1) *One of the issues raised during the Subcommittee's hearing was that some federal courts have not permitted defendants to argue that the information was not properly classified. What changes would you recommend to the existing statutes to take into account the fact that the modern classification system post-dates the enactment of the espionage act statutes?*

I would recommend two specific changes: *First*, the espionage statutes should generally be revised to prohibit the disclosure of "classified" information, as opposed to its current prohibitions of more ambiguous types of governmental material, including, for example, "information relating to the national defense." With regard to identifying classified information, the specific statutory language I would recommend would be to prohibit the disclosure of information that has been "classified pursuant to an Act of Congress or executive order relating to classification."

Second, I believe that the espionage statutes should be revised to take into account the possibility that the wrongfully disclosed information was, in fact, improperly classified. Such revisions could perhaps include the formal codification of an "improper classification" defense, which would allow defendants to prove at trial that the information they disclosed was not properly classified either pursuant to the relevant statute or the relevant Executive Order.

WASHINGTON COLLEGE OF LAW
4801 MASSACHUSETTS AVENUE, NW WASHINGTON, DC 20016
Phone: 202/274-4241 | Fax: 202/274-0830
E-Mail: svladeck@wcl.american.edu

63582.007

To be sure, I suspect that many would criticize such an amendment as providing an incentive to those in possession of information they believe to be wrongfully classified to disclose first, and face the consequences later. But even if government employees were willing to take such an extreme risk (i.e., willfully violating the Espionage Act and subjecting themselves to prosecution on the assumption that their defense would be successful), it might be possible to ameliorate this concern by requiring that the defendant have exhausted available *internal* remedies for challenging the classification before disclosing it publicly.

I don't mean to simplify things—this, to me, is the hardest single question that arises in the context of reforming the Espionage Act. But at the very least, I think that any attempt to revise the Espionage Act must take into account the documented problems with the current classification regime, and the reality that a substantial amount of information that might otherwise fall within the scope of the current Espionage Act is, in fact, wrongfully classified under section 1.7(a) of Executive Order 13,292, which provides that, "[i]n no case shall information be classified in order to: (1) conceal violations of law, inefficiency, or administrative error; (2) prevent embarrassment to a person, organization, or agency; (3) restrain competition; or (4) prevent or delay the release of information that does not require protection in the interest of the national security."

2) *If the Congress sought to limit the reach of the espionage statutes to only classic espionage cases as part of an effort to comprehensively legislate with respect other kinds of conduct, and using 18 U.S.C. § 793(d) and 793(e) as examples, please identify the changes that you think should be made to narrow the scope of these statutes to only address classic espionage cases.*

As I suggested at the hearing, if Congress sought to limit the scope of the espionage statutes to what we might colloquially understand as "classic" espionage cases (recognizing that Congress might elsewhere deal with leaking and whistleblowing), the easiest and most significant way to so narrow the statutes would be to codify a specific intent requirement. Thus, §§ 793(d) and (e), in particular, could be amended to require that the acts be undertaken "with the specific intent either to harm the national security of the United States or to benefit a foreign power." Of course, such intent could be inferred, in appropriate cases, from the conduct of the defendant. But requiring proof of such intent would eliminate the possibility that individuals could be subject to liability under the Espionage Act for non-espionage-motivated (albeit still prohibited) disclosures of national security information.

There are other possibilities as well, including focusing more specifically on the nature of the disclosure, the identity of the individual to whom the information is disclosed, and so on. But if the goal is simply to narrow the current regime to only

VerDate Nov 24 2008 14:12 Feb 07, 2011 Jkt 063582 PO 00000 Frm 00035 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\63582.TXT SJUD1 PsN: CMORC

63582.008

cover classical espionage, my own considered view is that a specific intent requirement would do virtually all of the necessary work.

* * *

I hope these answers are responsive to Senator Cardin's questions, and stand ready to assist you and your colleagues on the Committee if there is any additional information that I can provide.

Sincerely yours,

Stephen I. Vladeck

VerDate Nov 24 2008 14:12 Feb 07, 2011 Jkt 063582 PO 00000 Frm 00036 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\63582.TXT SJUD1 PsN: CMORC

63582.009

Questions for the Record from the Senate Committee on the Judiciary,
Subcommittee on Terrorism and Homeland Security Hearing,
"The Espionage Statutes: A Look Back and A Look Forward"

Question from Senator Cardin

During the Subcommittee hearing, reference was made to the *Rosen and Weissman* case. In that case, the District Court held that the government was required to prove, in a prosecution involving the transmittal of *intangible* "national defense information" under section 793(e), that the defendant had reason to know that the information he or she transmitted could harm the United States. What is your view as to the impact of the lower court's ruling on the government's ability to prosecute: (a) classic espionage cases; and (b) cases involving government employees or private persons who may have motives other than intending to harm the United States or aid a foreign country?

Response from Ken Wainstein

The District Court in United States v. Rosen and Weissman issued two rulings that could raise the government's burden in a leak prosecution. First, the Court required the government to show that the defendant *knew* that disclosure of the information he allegedly leaked was potentially harmful to the United States. This added to the statutory element in a case involving the disclosure of intangible (oral) national defense information that the defendant "ha[d] reason to believe [that information] could be used to the injury of the United States or to the advantage of any foreign nation." Second, the Court decided that in a case involving conspiracy to leak intangible national defense information, the defendant can be found guilty only if he "*intended* that such injury to the United States or aid to a foreign nation result from the disclosures."

Were these additional elements required by the judge in U.S. v. Rosen and Weissman to be applied in other cases, there would be an impact on the government's ability to prosecute under the espionage statutes. The impact would probably not be that significant in cases involving classic espionage, as the government typically has strong evidence that the defendant knew and intended that his disclosure would injure the United States and aid a foreign government.

The impact could be significant, however, in the prosecution of cases involving the leak of classified information from a government employee to the media, the type of case that was the focus of our May 12, 2010 hearing. The government may be able to surmount the first additional element and prove that a government employee charged with such a leak knew that the disclosure was potentially harmful to the United States. It could often do that by eliciting testimony that the classification system is based on potential harm to the United States and that the defendant employee received instruction or training to that effect.

The real difficulty arises with the second requirement imposed in the Rosen and Weissman case -- that the defendant intended to injure the United States or aid a foreign

63582.010

nation with the disclosure to the media. As we discussed at the hearing, media leakers are often motivated by interests having nothing to do with injuring our government or aiding another. Some are motivated, for example, by the feeling of self-importance they derive from showing others they are in the know, while others might be leaking information out of a genuine desire to improve the government by exposing and righting a perceived wrong in the government's operations -- both motives that would likely not satisfy the intent element in the Rosen and Weissman case. In the latter case, for example, the leaker is acting based on his perception that disclosure will enhance, rather than injure, the interests of the United States. As a result, the prosecution of such a leaker will be handicapped if the government has to prove that he intended to harm the U.S. or aid a foreign nation, with the result that the already challenging cases involving media leaks will become even more difficult to prosecute.

63582.011

SUBMISSIONS FOR THE RECORD

OPENING STATEMENT OF

SENATOR BENJAMIN L. CARDIN

CHAIRMAN, TERRORISM AND HOMELAND SECURITY SUBCOMMITTEE OF THE SENATE JUDICIARY COMMITTEE

HEARING: THE ESPIONAGE STATUTES: A LOOK BACK AND A LOOK FORWARD

WEDNESDAY, MAY 12, 2010

The subcommittee will come to order.

The current statutory framework with respect to the espionage statutes is a patchwork that traces its roots to the Espionage Act of 1917, which targeted classic espionage situations involving persons working on behalf of foreign nations. Constructed during the First World War, the current framework was formed at a time when intelligence and national security information existed primarily in some tangible form, such as blueprints, photographs, maps, and other documents. Our nation, however, has witnessed dramatic changes to nearly every facet of our lives over the last 100 years, including technological advances which have revolutionized our information gathering abilities as well as the mediums utilized to communicate such information.

VerDate Nov 24 2008 14:12 Feb 07, 2011 Jkt 063582 PO 00000 Frm 00039 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\63582.TXT SJUD1 PsN: CMORC

63582.012

Yet, the basic terms and structure of the espionage statutes have remained relatively unchanged in the nearly one hundred years since their inception. Moreover, the current statutory framework with respect to espionage was designed to address classic spy cases involving persons who intended to aid foreign governments. Issues have arisen in the investigation and defense of criminal cases when the statutes have been applied to other groups such as private citizens seek to obtain and disclose classified information, or when government employees disclose classified information, for purposes other than to aid a foreign government.

Legal scholars and commentators have criticized the current statutory framework as confusing and unwieldly, and have asked questions such as what Congress intended when it enacted the statutes because the language that is contained in the statutes could be read differently than Congress may have intended. Indeed, over the years, some federal courts have read additional elements into these offenses to uphold their constitutionality. One federal court observed in 1988 that "carefully drawn legislation" was a "better long-term resolution" than judicial intervention, and in 2006, a federal court in the Eastern District of Virginia observed that the "time is ripe" for Congressional review of the espionage statutes.

VerDate Nov 24 2008 14:12 Feb 07, 2011 Jkt 063582 PO 00000 Frm 00040 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\63582.TXT SJUD1 PsN: CMORC

63582.013

The jurisdiction of this Subcommittee includes "oversight of espionage laws and their enforcement," and this Subcommittee has not recently examined these issues. As a result, the purpose of this hearing is to take a look back at the espionage statutes, to examine how they have been used over the last 70 years, to examine what problems have developed, and to examine how the courts have dealt with these issues. The hearing is designed to educate us on these issues as well as to identify the policy and legal factors that the Congress should consider if it decides that changes might be appropriate.

The purpose of this hearing is not, however, to look at potential legislation such as media shield legislation or to focus on whether members of the press can be prosecuted. Those issues have been dealt with in other hearings and legislation has already been considered by the full Judiciary Committee. Rather, this hearing is focused on the application of the espionage statutes to groups such as private persons and government employees, who may have motives and intent other than to aid foreign governments, as well as to classic spy cases.

VerDate Nov 24 2008 14:12 Feb 07, 2011 Jkt 063582 PO 00000 Frm 00041 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\63582.TXT SJUD1 PsN: CMORC

63582.014

We have a distinguished panel of witnesses to testify at today's hearing, who will be presenting a wide range of viewpoints. I look forward to hearing their testimony. I will now recognize Senator Kyl, the Ranking Member of our Subcommittee, for any remarks that he would care to make at this time.

VerDate Nov 24 2008 14:12 Feb 07, 2011 Jkt 063582 PO 00000 Frm 00042 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\63582.TXT SJUD1 PsN: CMORC

63582.015

"The Espionage Act: A Look Back and a Look Forward"

12 May 2010

SUBCOMMITTEE ON TERRORISM AND HOMELAND SECURITY
SENATE JUDICIARY COMMITTEE

Senator Jon Kyl

Introduction

At the outset, I would like to thank Chairman Cardin for holding this hearing to examine the effectiveness of the espionage laws.

Throughout my years on this Subcommittee, I have worked to ensure that the law keeps pace with changes in technology and national security needs. At this hearing, we have the opportunity to examine statutes reaching back to the early 1900s to ensure that they are appropriate to the challenges of today.

Leaks of Classified Information

Leaks of classified information are a grave matter and a serious problem. This might seem like an obvious point, but many people seem to think that leaking classified information is justified in some circumstances, such as when leaking it to a reporter rather than to a spy. There are two rationales that are sometimes advanced to distinguish a media leak from traditional espionage behavior. As I will explain, neither of these rationales is compelling.

First, some have suggested that leaking information, especially to the press, is a legitimate form of "whistle-blowing" by government employees. To be sure, there are situations where whistle-blowing is appropriate. It is important, for example, that government employees have the ability to bring illegal activity to the light of day. But there is a right way, and a wrong way, for government employees to raise concerns that misconduct or illegal activity has occurred. Congress has passed whistle-blower statutes that provide mechanisms for employees to report activities without compromising sensitive or classified information, and employees should take full advantage of the protections that those statutes provide. When an employee decides instead to go outside

63582.016

those approved channels by leaking classified information to the press, he or she should be prosecuted.

Second, some argue that a person's motives for disclosing classified information should play a role in determining whether the individual can be prosecuted. Again, this is not a compelling argument. Whether one discloses classified information to intentionally harm the United States or for some other reason, such as fame, the deleterious effect on national security remains the same. Indeed, "well intentioned" leaks to the press can be more harmful than a traditional espionage leak—instead of exposing U.S. secrets to a single country, they make them available to the entire world. The fact is that all government employees with access to classified information agree not to disclose or share it with unauthorized persons. An individual who intentionally does so anyway should be held accountable, no matter whether his "motive" is to harm the United States or not.

A prime example in the classic espionage context is Jonathan Pollard, the Israeli spy who received a life sentence in 1987. According to reports, Pollard never revealed the names of U.S. agents or military plans. And in a memorandum to his sentencing judge he said, "I never thought for a second that Israel's gain would necessarily result in America's loss. How could it?" Notwithstanding these seemingly innocent motives, Pollard was—rightfully, in my opinion—punished severely for abusing the trust placed in him by the American people. Those who leak classified information to the press are similarly abusing their positions of trust.

Past Attempts at Reform

Although it appears that the espionage statutes generally work well at permitting the prosecution of government employees and others who are accused of spying (such as Jonathan Pollard), the statutes might not work as well in a leak context where the accused is not a foreign agents and/or did not intend specifically harm to the United States.

In 2000, in an attempt to update the statutes, Congress passed a measure to criminalize all unauthorized leaks of classified information.[1] It would have made it easier for the government to prosecute unauthorized disclosures of classified information by eliminating the need to *prove* that

[1] H.R. 4392 § 303, 106th Congress.

VerDate Nov 24 2008 14:12 Feb 07, 2011 Jkt 063582 PO 00000 Frm 00044 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\63582.TXT SJUD1 PsN: CMORC

63582.017

damage to national security has resulted or would result from the unauthorized disclosure, requiring instead only that the unauthorized disclosure was of information properly classified under a statute or executive order. President Clinton vetoed the measure, asserting that it was too broad and posed a risk of "unnecessarily chill[ing] legitimate activities that are at the heart of a democracy."[2]

Courts have continued to struggle with the existing statutory framework in attempting to adapt it to the cases at hand. The espionage statutes have been criticized as being "unwieldy and imprecise instruments."[3] In a recent case[4] involving access to classified information, after noting that that "the basic terms and structure of this statute have remained largely unchanged since the administration of William Howard Taft" and that "[t]he intervening years have witnessed dramatic changes in the position of the United States in world affairs and the nature of threats to our national security," the court stated that Congress should engage in a "thorough review" of these statutes.[5] I am pleased that we are doing that today.

More Modest Reforms

Separate from past attempts to make major reforms in this areas, several of our witnesses have suggested some relatively straight-forward changes that could help modernize the espionage statutes. For example, one could clarify that electronic information is protected by the statutes. And the statute could be amended to protect information relating to "national security" (currently, the statute protects information relating to the "national defense"). I look forward to hearing what our witnesses have to say about these potential changes.

I also look forward to hearing our witnesses testify about the role of Classified Information Procedures Act in prosecuting espionage and leak cases. One of the reasons that we don't see more leak prosecutions is because these cases often require the government to reveal additional classified information during the course of the trial. Thus, the government is often forced to choose between bringing leakers to justice and protecting national security information. CIPA is supposed to help protect this information, but unfortunately it has a relatively mixed record of effectiveness.

---

[2] Statement by the President to the House of Representatives, 36 WEEKLY COMP. PRES. DOC. 278 (Nov. 4, 2000).
[3] *United States v. Morison*, 844 F.2d 1057, 1086 (4th Cir. 1988) (Phillips, J., concurring).

[4] *United States v. Rosen*, 445 F.Supp. 2d 602 (E.D. Va. 2006).
[5] *Rosen*, 445 F. Supp. 2d at 646.

VerDate Nov 24 2008 14:12 Feb 07, 2011 Jkt 063582 PO 00000 Frm 00045 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\63582.TXT SJUD1 PsN: CMORC

63582.018

Last year, I introduced legislation that would implement some common-sense fixes to CIPA. I believe that these fixes would make CIPA more effective at protecting information and might allow prosecutors to bring cases that they otherwise would not. I am interested in getting the panel's views on these proposals.

Conclusion

I hope that today's hearing will serve as a springboard for a continuing dialogue about how Congress can best help to protect classified information.

I look forward to hearing from the witnesses.

Thank you, Mr. Chairman.

VerDate Nov 24 2008 14:12 Feb 07, 2011 Jkt 063582 PO 00000 Frm 00046 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\63582.TXT SJUD1 PsN: CMORC

63582.019

McDermott
Will & Emery

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

May 7, 2009

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

VIA EMAIL AND FIRST CLASS MAIL

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

Re: Hearings On The Espionage Act of 1917

Dear Chairman Cardin:

I appreciate your invitation to address some of the issues raised by The Espionage Act of 1917 ("the Act") for which you are holding hearings. My involvement with the law and its related statutes (e.g., the Classified Information Protection Act) stems from my time working in the Department of Justice as Special Assistant to the Attorney General (when CIPA was first drafted and enacted) and in my criminal defense practice (I was one of the attorneys in the so-called American-Israeli Public Affairs Committee [AIPAC] case and am working on an active Espionage Act investigation now).

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

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

U.S. practice conducted through McDermott Will & Emery LLP.
500 Thirteenth Street, N.W. Washington, D.C. 20005-3096 Telephone: 202.756.8000 Facsimile: 202.756.8087 www.mwe.com

63582.020

One problem with any law that addresses the improper disclosure of classified information, of course, is the over-classification of information. I realize this is not an issue the Committee is addressing, but it is an important consideration when a law criminalizes disclosure of such material. As many others have indicated, "when everything is classified, nothing really is classified." Any law would work best if applied to a system that carefully distinguished between that information that should be closely held and that which may be confidential from a policy or political point of view, but not from the perspective of national security. Too often, government officials during their day's work find it easier to classify information or classify it at a higher level than necessary because it requires more effort and consideration to do less. In any event, this is an issue for another time.

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

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

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

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

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

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

- As the law requires that disclosures are made to people who are "not authorized" to receive it, how do government officials know when they are talking to the media the occasions when "leaks" are what their superiors want or have done themselves versus when they are violating the rules?

- The law speaks of tangible things – maps, documents, etc. – and yet can it possibly be applied when government officials and others (including the media) just discuss things that they normally do as part of their jobs (and in those conversations touch on information that is contained in a document or other tangible object somewhere)?

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

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

The AIPAC case itself is a good vehicle for the Committee to analyze the Act. In that case, for reasons that we still do not know, counter-intelligence and/or law enforcement agencies began following and investigating AIPAC employees in their dealings with U.S. government and Government of Israel officials for years. These AIPAC foreign policy experts were relied on by U.S. government officials for information and they, in turn, did their jobs of advising AIPAC and others in the community based on their government interactions. The AIPAC people did not have confidentiality agreements with the government, were not given security clearances to do their work, and were never told (except in a DOJ sting) that they should not be hearing what they were hearing. Nevertheless, not only were these two individuals (Steven Rosen and Keith Weissman) investigated, they were charged with violating The Espionage Act of 1917. Before the actual charges were filed, in meetings with the Justice Department, government attorneys even raised the possibility that the two could be charged under the most severe section of the statute (18 U.S.C. § 794) for which the punishment included the death penalty.

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

That the same section or sections of the Act can be used to prosecute this conduct along side with former FBI agent turned Russian spy Robert Hannsen shows that the statute both sweeps too broadly and also does not properly address the real conduct it seeks to make criminal. The Act's breadth and vagueness can, in the hands of ill-intended investigators and prosecutors, result in a powerful chill on the kinds of open government, freedom of the press, and transparency in proper foreign policy formulation that makes this country stronger. It does not serve proper national security or law enforcement interests to have this possibility of improper

application of the Act to conduct that was not targeted in 1917 and has even less reason to be targeted today.

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

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

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

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

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

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

6) define the *mens rea* required for each offense in terms that are clear so people can conform their conduct and judges and juries can apply the law evenly and consistently when it is violated;

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

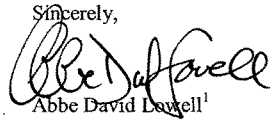
8) make clear how the law covers tangible as well as non-tangible information in a manner that protects First Amendment activity and whether and how, in the

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

There is a great deal of case law that can instruct this oversight exercise. However, courts have been constrained to use the existing structure and language of the statute in applying it. Obviously, Congress is not so limited. The point is that there is a real opportunity that your hearings recognize to create a tough law, a clear law, and a law that also can respect the values we place on a free speech and open government.

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

Sincerely,



Abbe David Lowell[1]

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

Testimony of Jeffrey H. Smith

Subcommittee on Terrorism and Homeland Security

Committee on the Judiciary, U.S. Senate

May 12, 2010

Mr. Chairman, Senator Kyl, thank you for the opportunity to speak with you this morning on the very important question of whether Congress should consider revising the espionage statutes in light of recent court decisions and the current threats we face. In a word, I believe the answer is "yes" - but any revisions must be very carefully considered, as these statutes touch on our core values and national security.

The Subcommittee has asked this panel to "look back and look forward" and therefore I thought it would be useful to begin by asking what role the criminal law should play in protecting the nation's most important secrets. The world has changed enormously since the predecessor of the espionage statutes was enacted in 1911. Yet much of the original language survives to this day. To a modern ear, it sounds antiquated. The threats of today are vastly different and more complex than those we faced in the First World War. The question before the Subcommittee, then, is whether the various espionage statutes, particularly 18 U.S.C. §§ 793 and 794, should be revised in light of all of the changes that have occurred since 1911 and the threats we currently face.

I have been privileged to serve in the Pentagon, the Department of State, on the Senate Staff (as General Counsel of the Senate Armed Services Committee) and as General Counsel of the CIA. In all of these positions, I have encountered issues associated with the protection of classified information, the espionage statutes, real spies, and lots of "leaks" of classified

VerDate Nov 24 2008 14:12 Feb 07, 2011 Jkt 063582 PO 00000 Frm 00052 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\63582.TXT SJUD1 PsN: CMORC

63582.025

information. In private practice it has been my privilege to represent news media organizations and individual reporters on these issues and, in one instance, a former government employee who faced possible charges for violating the espionage statutes. These experiences will inform my testimony this morning and I hope will help the Subcommittee with its review of these statutes.

It is often said that the first responsibility of our government is to provide for the security of its citizens. Doing so means that some information must necessarily be kept secret - from our adversaries and from public disclosure. Our system vests primary responsibility to determine what information should be kept secret in the President. Over the years, Presidents have adopted a series of executive orders spelling out the requirements for classifying information, the unauthorized disclosure of which could be expected to cause damage to our national security. Information is sometimes classified that should not be, but no one seriously questions that the government does have real secrets that must be protected and that prosecution is an appropriate tool to use to protect those secrets. However, there are serious and difficult questions as to how widely the criminal law should sweep in protecting secrets.

In my testimony this morning, I will, for ease of discussion use "properly classified information" as synonymous with "secret," although that is not without debate, as I'll touch on later.

There is wide agreement that a government employee or contractor who has authorized access to properly classified information who knowingly gives or sells the information to an agent of a foreign power should be prosecuted. Similarly, a person acting on behalf of a foreign power who seeks to obtain, or does obtain, properly classified information without authority should be prosecuted. These are the classic spy cases - the Aldrich Ames, Robert Hansens, John Walkers and Colonel Abels of this world.

VerDate Nov 24 2008 14:12 Feb 07, 2011 Jkt 063582 PO 00000 Frm 00053 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\63582.TXT SJUD1 PsN: CMORC

63582.026

However, when we move beyond these cases the questions become more difficult. The unauthorized disclosure of properly classified information to persons who are not foreign agents, for example to the press, plunges us immediately into a tangled web of competing national interests. And it is those competing interests that the courts and Congress have struggled with over the years.

I commend the Subcommittee for taking up these very difficult questions. As you know, a highly respected federal district judge, Judge T.S. Ellis III, in an August 2006 opinion in the "AIPAC" case urged the Congress to "engage in a thorough review and revision of [the espionage statutes] to ensure that they reflect both [the changes that have occurred since the statutes were first enacted] and contemporary views about the appropriate balance between our nation's security and our citizens' ability to engage in public debate abut the United States' conduct in the society of nations." *United States v. Rosen*, 445 F. Supp. 2d 602, 646 (E.D. Va. 2006).

I believe the Subcommittee should take up Judge Ellis' invitation. The espionage statutes need a careful review. However, care must be taken because the statutes have served us well, particularly in our ability to prosecute real spies. That ability must be preserved and, if possible, strengthened. The Subcommittee can be confident that government employees who have access to properly classified information have no doubt that if they pass such information to a foreign power and get caught, they are going to jail. It is an effective deterrent. That said, I have a few modest suggestions that I believe should be considered to make prosecution of real spies easier. I will discuss those suggestions shortly.

However, the more difficult questions are presented as we move beyond the spies and seek to use the espionage statutes to prosecute those who "leak" properly classified information

VerDate Nov 24 2008 14:12 Feb 07, 2011 Jkt 063582 PO 00000 Frm 00054 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\63582.TXT SJUD1 PsN: CMORC

63582.027

to the press or others outside the government who are not foreign agents but who do not have authorized access to the information. It is these "leak" cases that present the hardest questions. And, by contrast to the risk of prosecution for passing secrets to a foreign power, government employees who leak to the press are much less deterred by the law.

Before turning to those issues, let me give you some thoughts on how I believe the existing statutes can be modernized to making prosecuting real spies easier. My suggestions are tentative and clearly need to be thoroughly considered by Congress before they are enacted; but I believe they should be considered.

I. Suggestions for Modernizing the Espionage Statutes

A. Forms of Information

First, the statutes, 18 U.S.C. §§ 793 and 794, speak of "any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note relating to the national defense." Obviously these words predate the information age. I do not know, for example, what a "signal book" is and I am not sure the government even has such things anymore.

Over time, the courts have been able to interpret the statute to include information in various forms, but as information technology changes every eighteen months as "Moore's law" tells us, I think a change in the statute should be considered.

One approach is simply to replace the current list in sections 793 and 794 with the words "information in whatever form." I defer to my Department of Justice colleagues as to whether that is too vague. If so, another approach would be to add the words "electronic media or information in electronic form" to the list. I believe that would capture much if not all of the contemporary communications that should be protected. I am concerned that unless some

VerDate Nov 24 2008 14:12 Feb 07, 2011 Jkt 063582 PO 00000 Frm 00055 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\63582.TXT SJUD1 PsN: CMORC

63582.028

change is made we may face a situation in a few years in which this list of antiquated language makes prosecution of a serious espionage case difficult or perhaps impossible.

B. "Information Relating to the National Defense"

Second, those sections speak of "information relating to the national defense." As noted earlier, the Executive Order on protecting classified information, Exec. Order. No. 13526, signed by President Obama on December 29, 2009, speaks of information relating to the "national security." The Executive Order defines "national security" as "the national defense or foreign relations of the United States." Exec. Order No. 13526, Section 6.1(cc). In my view, the scope of the information sought to be protected for national security purposes is correctly set out in the executive order - it is not merely "defense information" in the plain meaning of those words. Courts have recognized that and over time, as Judge Ellis points out in his August 2006 opinion,

> "the phrase 'information relating to the national defense' has consistently been construed broadly to include information dealing with military matters and more generally with matters relating to United States foreign policy and intelligence capabilities."

United States v. Rosen, 445 F. Supp. 2d at 620.

That's true, but it's not been without some contortions along the way. I suggest that the subcommittee consider replacing the term "national defense" with the term "national security" and adopting a definition similar to that in the executive order.

The advantage of adopting the term "national security" is that it reflects the broader range of issues that deserve to be protected in our national security interest. These range from foreign policy to international economic issues, from border security to drug trafficking, In each of these areas there are true national security secrets that need to be protected and the disclosure of them should be a crime.

VerDate Nov 24 2008 14:12 Feb 07, 2011 Jkt 063582 PO 00000 Frm 00056 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\63582.TXT SJUD1 PsN: CMORC

63582.029

In the past, courts have, as Judge Ellis said, been able to interpret the term "national defense" with sufficient breadth to cover many of these issues, but that has sometimes required the government to link a series of documents or acts to ultimately find some nexus to defense or military interests. For example, I was the lawyer at the Department of State during the prosecution of Truong Dinh Hung, who obtained classified diplomatic cables from a Department of State employee and then passed them to the communist government of Vietnam. He gave them vast numbers of highly classified cables and other documents that dealt with a wide range of foreign policy issues. *See United States v. Truong Dinh Hung*, 629 F.2d 908 (4th Cir. 1980). Yet we and the Department of Justice had to look hard to identify documents he had given to the Vietnamese that could be used in the indictment and trial that were not "pure" foreign policy discussions (for example, discussions of U.S.-China relations) but rather dealt with something much closer to a traditional military issue. We were successful, but the prosecution would have been much easier if we had not had to stitch together a number of documents in order to convince the jury and the court that his espionage related to the "national defense."

In my view, adopting national security as the standard reduces the risk that some future prosecution of an individual would fail because the government was not able to prove that the disclosure - however harmful to the national security - was not "related to the national defense."

I recognize this proposal will cause concern that the definition is too broad and sweeps in matters that, while sensitive, should not be dealt with by the criminal law. Some will argue that adopting a term used in the executive order gives the President authority to classify information that should not be classified, thus making disclosure of that information a crime. This risk is avoided, it seems to me, by the requirement in current law that the government must prove that the defendant knew or had reason to believe that the information could be used to the injury of

VerDate Nov 24 2008 14:12 Feb 07, 2011 Jkt 063582 PO 00000 Frm 00057 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\63582.TXT SJUD1 PsN: CMORC

63582.030

the United States or to the advantage of any foreign nation. The courts will surely give great weight to the executive branch determination that the information is properly classified and the disclosure has caused, or is likely to cause, harm to the national security. But, the mere act of classification would not be sufficient. The harm must be proved in court to get a conviction.

C. "Foreign Nation"

Third and in a similar vein, I suggest that the term "foreign nation" in sections 793 and 794 be changed to "foreign power" and defined substantially as it is defined in the Foreign Intelligence Surveillance Act - *e.g.*, to include a faction of a foreign nation and terrorist groups. *See* 50 U.S.C. § 1801. As the Subcommittee knows, the government must prove that the defendant had "reason to believe" the information conveyed could be used to the injury of the United States "or to the advantage of any foreign nation." Given that many of the threats we face today come not from nation states, but from terrorist groups and other non-state actors it seems prudent to avoid any potential problems in a future prosecution by making clear in the law that the statute applies equally to a nation state and non-state actors who are a threat to our national security. I am not aware that the current language has been a problem in this respect, but I believe this change merits careful consideration.

II. Prosecution of Those Who "Leak" Classified Information to the Media

Let me now turn to the more difficult issues associated with the espionage statutes - namely the prosecution of those who "leak" classified information to the media and those in the media who publish it. Here, I encourage the Subcommittee to review the statutes, as Judge Ellis suggested, but I urge great caution in doing so. Leaks have caused great damage; but caution is needed because the efforts to get at this problem through legislation in the past have failed and

VerDate Nov 24 2008 14:12 Feb 07, 2011 Jkt 063582 PO 00000 Frm 00058 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\63582.TXT SJUD1 PsN: CMORC

63582.031

there is a risk that in seeking to make improvements we make the situation worse. Let me try to explain.

As I said, every Administration in which I have served has suffered from leaks that have been truly harmful. And every Administration has struggled to solve the problem but none have had much success.

The most recent example was the "Shelby Amendment" in 2000 and 2002 that would have added a new provision to 18 U.S.C. § 798 making it a crime for a government employee or former employee to disclose "any classified information" to an unauthorized person. The focus was on the person who leaked the information, not on the reporter or on the media who published it.

Congress passed this seemingly straightforward provision as part of the Intelligence Authorization Act for FY 2001 but after intense opposition from a wide range of groups and individuals, President Clinton vetoed the bill and Congress subsequently stripped out the provision. In his veto message, President Clinton said the provision would "unnecessarily chill legitimate activities that are the heart of a democracy." Message on Returning Without Approval to the House of Representatives the "Intelligence Authorization Act for Fiscal Year 2001," 36 Weekly Comp. Pres. Doc. 278 (Nov. 4, 2000). He spoke further of government officials fearing they "could become the subject of a criminal referral for prosecution" as a result of "engaging even in appropriate public discussion, press briefings or other legitimate official activities." *Id.*

President Clinton's veto was, in my view, an acknowledgment that senior government officials talk frequently to the press - often on "background" and with authorization - and provide information that is, in fact, classified. However, they do so anonymously and without taking the formal steps to declassify the information. These authorized backgrounders are held

VerDate Nov 24 2008 14:12 Feb 07, 2011 Jkt 063582 PO 00000 Frm 00059 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\63582.TXT SJUD1 PsN: CMORC

63582.032

in the genuine belief that the information should be made public - but not officially. The reasons vary widely, but often as a trial balloon for a policy change or to signal an important foreign policy objective to other nations. In my experience, these background briefings are typically approved at the highest levels and with the best interests of the United States at heart. The problem, of course, is that the information that was given to the press remains classified in the sense that the government documents that contain the very information disclosed to the press "on background" remains marked and handled as classified.

As laudatory as this practice might be from the point of view of informing the public, it clearly presents problems for the protection of classified information. For example, if the Secretary of State directs that the press be "backgrounded" on an upcoming meeting of foreign ministers, there must be a decision as to how much the press is to be told. Typically, some highly sensitive information is not given to the press because the Secretary knows that if that were to become public it would harm American interests.

However, enterprising journalists who got the "backgrounder" will call around to their other sources and are often able to discover the sensitive information that the Secretary did not want released. The reason is because the reporter's source is not likely to know that there had been an authorized backgrounder or does not know what information the Secretary doesn't want disclosed, but quickly realizes that someone else is talking so does not feel constrained in discussing the matter with a reporter. The source may also disagree with the policy and want to get his or her views out.

In other words, putting out sensitive information to the press - even in a controlled fashion - may be a legitimate effort to inform the public, but an administration can hardly be surprised when, having permitted the press to pull on the first thread, the whole sweater unravels.

VerDate Nov 24 2008 14:12 Feb 07, 2011 Jkt 063582 PO 00000 Frm 00060 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\63582.TXT SJUD1 PsN: CMORC

63582.033

And this is where the question of using the criminal law to punish the "unauthorized leak" as compared to the "authorized leak" is problematic and indeed troublesome.

The matter was considered again in 2001 as part of the 2002 Intelligence Authorization Act, but Congress instead included a provision requiring the Attorney General to "carry out a comprehensive review of current protections against the unauthorized disclosure of classified information." Pub. L. No. 107-108, § 310 (2001). Attorney General Ashcroft submitted his report in October of 2002. It is, I believe, a very thoughtful discussion of these issues. Mr. Ashcroft wrote that:

> Given the nature of unauthorized disclosures of classified information that have occurred, however, I conclude that current statutes provide a legal basis to prosecute those who engage in unauthorized disclosures, if they can be identified. It may be that carefully drafted legislation specifically tailored to unauthorized disclosures of classified information generally, rather than to espionage, could enhance our investigative efforts. The extent to which such a provision would yield any practical additional benefits to the government in terms of improving our ability to identify those who engage in unauthorized disclosures of classified information or deterring such activity is unclear, however.

Letter from Attorney General John Ashcroft to Speaker of the House of Representatives J. Dennis Hastert (Oct. 15, 2002).

He then went on to suggest a range of measures that the administration was taking or planning to take to prevent the unauthorized disclosure of classified information and the identification and punishment, either by prosecution or administrative action, of persons who disclose classified information without authority. I believe his recommendations were sound and I urge this Subcommittee to revisit the Ashcroft letter and ask the current administration to determine what measures recommended by Attorney General Ashcroft have been adopted and what the results have been.

VerDate Nov 24 2008 14:12 Feb 07, 2011 Jkt 063582 PO 00000 Frm 00061 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\63582.TXT SJUD1 PsN: CMORC

63582.034

As the Subcommittee considers whether the espionage statutes should be modernized, I suggest that the focus be – as was the Shelby Amendment and the Ashcroft letter – on those who have authorized access to classified information. They, after all, possess the information in the first place and they have a special responsibility to protect it. Those who become real spies should be prosecuted with the full might of the government. Those who, without authority, leak to the media or others not authorized to have possession of classified information should similarly be prosecuted. In the case of unauthorized leaks, the first problem is always to find them. Mr. Ashcroft had some good suggestions that I believe would help track down the leakers.

I do not believe that a major effort to revise the espionage statutes to make it "easier" to prosecute the media would be productive. I note that several courts, including the Supreme Court and most recently Judge Ellis, have intimated that journalists could be prosecuted. There has never been a prosecution of a journalist for publishing classified information and I am not sure that it is wise to open up the statutes in an effort to facilitate prosecution of journalists. There are many reasons for this, including the obvious first amendment issues that are raised. But another issue is that journalism is changing so fast these days with blogs and the like that it would be very difficult, if not impossible, to draft a statute that would improve the protection of real secrets without raising additional problems that are nearly impossible to predict.

But let us be clear. Leaks cause great harm and I encourage the Subcommittee and the executive branch to work together to find ways to reduce harmful leaks. In my mind, the most important step is greater discipline in the executive branch in four areas:

- First, classify only that information that truly requires protection in the national security interest. The President's new Executive Order takes some important steps in this direction.

VerDate Nov 24 2008 14:12 Feb 07, 2011 Jkt 063582 PO 00000 Frm 00062 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\63582.TXT SJUD1 PsN: CMORC

63582.035

- Second, make clear that leaks will not be tolerated and when they occur, investigate and prosecute those who leaked vigorously. Every Administration tries to do this; I know it's hard but it must be done.
- Third, do not abuse the practice of backgrounding the press. When a decision is made to do so and it involves discussing classified information, make clear to others that the press has been briefed and consider declassifying those portions that have been discussed with the press so that the remaining information is still classified – and people know what is, and what is not, classified.
- Fourth, because many leaks come from individuals who disagree with policy or otherwise believe that some information should be made public, urge greater use of hotlines or "dissent channels" to permit these individuals to make their concerns known up the chain of command - or even to Congress - so they are not tempted to go to the press in order to make their views known.

Ultimately, Mr. Chairman, the government does have secrets that must be protected. Our national security often depends on our ability to protect those secrets and that includes vigorous enforcement of the laws that penalize unauthorized disclosures that truly cause harm. But there are also other interests that must be taken into account in our democracy. The free flow of information between the government and the people, the transparency of government actions, the vigilance of a free press are also vital to our democracy and our freedom. Sometimes, as in the case of Aldrich Ames and Robert Hansen, the lines are very clear. In other cases, they are not. Perhaps the wisest observation on this issue I ever heard came from a law professor whom I greatly admired. When Daniel Ellsberg admitted that he was the source of the leak of the

VerDate Nov 24 2008 14:12 Feb 07, 2011 Jkt 063582 PO 00000 Frm 00063 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\63582.TXT SJUD1 PsN: CMORC

63582.036

Pentagon Papers to the New York Times, my professor said, "I know what to do; we should give him a medal and then send him to prison."

Mr. Chairman, I look forward to your questions.

VerDate Nov 24 2008 14:12 Feb 07, 2011 Jkt 063582 PO 00000 Frm 00064 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\63582.TXT SJUD1 PsN: CMORC

63582.037

THE ESPIONAGE ACT: A LOOK BACK AND A LOOK FORWARD
Hearing Before the Senate Committee on the Judiciary
Subcommittee on Terrorism and Homeland Security
Wednesday, May 12, 2010

Written Testimony of Stephen I. Vladeck
Professor of Law, American University Washington College of Law

Mr. Chairman, Ranking Member Kyl, and distinguished members of the Subcommittee:

Thank you for inviting me to testify today on such an important—but often neglected—topic. I suspect that we all have common cause when it comes to the need for harsh criminal sanctions for those who commit acts of espionage against the United States, and the Espionage Act of 1917 and its related statutes are vital in ensuring that the unauthorized disclosure of our national security secrets is not just prohibited, but severely punished.

And yet, as significant as the Espionage Act is (and has been), it is also marked by profound and frustrating ambiguities and internal inconsistencies. Attempting to distill clear principles from the state of the federal espionage laws in 1973, a pair of Columbia Law School professors—Hal Edgar and Benno Schmidt—lamented that, "the longer we looked, the less we saw." Instead, as they observed, "we have lived since World War I in a state of benign indeterminacy about the rules of law governing defense secrets."[1] If anything, such benign indeterminacy has only become more pronounced in the four decades since—and, according to some, increasingly less benign.

I. Statutory Background[2]

a. The Espionage Act

1. *See* Harold Edgar & Benno C. Schmidt, Jr., *The Espionage Statutes and Publication of Defense Information*, 73 COLUM. L. REV. 929 (1973).

2. This background discussion is taken from Stephen I. Vladeck, *Inchoate Liability and the Espionage Act: The Statutory Framework and the Freedom of the Press*, 1 HARV. L. & POL'Y REV. 219, 221–31 (2007).

VerDate Nov 24 2008 14:12 Feb 07, 2011 Jkt 063582 PO 00000 Frm 00065 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\63582.TXT SJUD1 PsN: CMORC

63582.038

From the Sedition Act of 1798 (which expired in 1801) through the outbreak of the First World War, there was virtually no federal legislation prohibiting seditious expression. Indeed, there were no general federal laws prohibiting the dissemination or publication of almost any information potentially harmful to the national defense. Contemporaneously with the United States's entry into the war, however, Congress enacted the Espionage Act of 1917, which, except for the amendments discussed below, remains on the books largely in its original form today at 18 U.S.C. §§ 793–99. Drafted principally by then-Assistant Attorney General Charles Warren, the Act includes a number of seemingly overlapping and often ambiguous provisions.

Current 18 U.S.C. § 793(a), which derives from section 1(a) of the Espionage Act, prohibits the obtaining of information concerning a series of national defense installations—places—"with intent or reason to believe that the information is to be used to the injury of the United States, or to the advantage of any foreign nation." Similarly, § 793(b) prohibits individuals with "like intent or reason to believe" from copying, taking, making, or obtaining "any sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, document, writing, or note of anything connected with the national defense." Although an early legal challenge argued that the requirement that the information at issue be "connected with the national defense" was unconstitutionally vague, the Supreme Court read a scienter requirement into the statute (and, so construed, upheld it) in *Gorin* v. *United States* in 1941.[3]

Section 793(c) is, in important ways, far broader. The descendant of section 1(c) of the original Espionage Act, this provision creates criminal liability for any individual who "receives or obtains or agrees or attempts to receive or obtain from any person, or from any

3. *See* 312 U.S. 19, 27–28 (1941) ("The obvious delimiting words in the statute are those requiring 'intent or reason to believe that the information to be obtained is to be used to the injury of the United States, or to the advantage of any foreign nation.'").

VerDate Nov 24 2008 14:12 Feb 07, 2011 Jkt 063582 PO 00000 Frm 00066 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\63582.TXT SJUD1 PsN: CMORC

63582.039

source whatever" various material related to the national defense, so long as the individual "know[s] or ha[s] reason to believe, at the time he receives or obtains [the information] ... that it has been or will be obtained, taken, made, or disposed of by any person contrary to the provisions of [the Espionage Act]." Thus, whereas §§ 793(a) and 793(b) prohibit the collection of secret information relating to the national defense, § 793(c) prohibits the receipt of such information, or even attempts at receipt thereof, so long as the recipient does or should have knowledge that the source, in obtaining the information, violated some other provision of the Espionage Act.

In addition, whereas §§ 793(d) and 793(f) prohibit the dissemination of national security information that is in the lawful possession of the individual who disseminates it (§ 793(d) prohibits willful communication; § 793(f) prohibits negligence), § 793(e)—which, like § 793(d) and 793(f), derives from section 1(d) of the Espionage Act—prohibits the same by an individual who has unauthorized possession of the information at issue.

Thus, in sweeping language, § 793(e) prohibits individuals from willfully communicating—or attempting to communicate—to any person not entitled to receive it:

> any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation.

Section 793(e) goes one important step further, however, for it also prohibits the retention of such information and the concomitant failure to deliver such information "to the officer or employee of the United States entitled to receive it." Section 793(e) therefore appears to have a far more relaxed intent requirement than § 793(a) and 793(b). The provision does not require specific intent so long as the communication or retention of classified information is "willful," a point on which I will elaborate below.

VerDate Nov 24 2008 14:12 Feb 07, 2011 Jkt 063582 PO 00000 Frm 00067 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\63582.TXT SJUD1 PsN: CMORC

63582.040

One of the important questions that has arisen with regard to § 793(e) is whether, and to what extent, it might apply to the press. Many have argued against the applicability of § 793(e) to the press because of the absence of an express reference to the "publication" of such secret national security information. In contrast, three separate provisions of the Espionage Act *do* expressly prohibit the *publication* of particular national defense information:

First, § 794(b) applies to "[w]hoever, in time of war, with intent that the same shall be communicated to the enemy, collects, records, publishes, or communicates ... [the disposition of armed forces] or any other information relating to the public defense, which might be useful to the enemy." Although the provision might appear to turn on whether it is a "time of war," a subsequently enacted provision—§ 798A—expands § 794(b) to apply so long as various national emergencies remain in place, a condition that remains satisfied today. Second, § 797 applies to whoever "reproduces, publishes, sells, or gives away" photographs of specified defense installations, unless the photographs were properly censored.

Third, § 798(a), which generally relates to cryptography and was passed in 1950 at least largely in response to the *Chicago Tribune* incident from World War II,[4] applies to whoever "communicates, furnishes, transmits, or otherwise makes available ... or publishes" various prohibited materials, including "classified information ... concerning the communication intelligence activities of the United States or any foreign government." Section 798(b) defines "classified information" as "information which, at the time of a violation of this section, is, for reasons of national security, specifically designated by a United States Government Agency for limited or restricted dissemination or distribution." Whether the

4. Shortly after the Battle of Midway, the *Chicago Tribune* ran a series of articles suggesting that the U.S. Navy had prevailed largely because it had prior warning of the location of the Japanese attack. Concerned that Japanese intelligence would correctly surmise that the Americans had broken Japanese naval codes, the government initiated criminal proceedings against the *Tribune*. Fearful that the prosecution would itself tip off the Japanese, though, the United States dropped the case. *See* Jeffery A. Smith, *Prior Restraint: Original Intentions and Modern Interpretations*, 28 WM. & MARY L. REV. 439, 467 (1987).

VerDate Nov 24 2008 14:12 Feb 07, 2011 Jkt 063582 PO 00000 Frm 00068 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\63582.TXT SJUD1 PsN: CMORC

63582.041

specific references to publication in these three sections exclude the applicability of other provisions of the statute to the press is an issue to which I shall return shortly.

One other noteworthy provision of the Espionage Act is 18 U.S.C. § 794(a), which applies to "[w]hoever, with intent or reason to believe that it is to be used to the injury of the United States or to the advantage of a foreign nation, communicates, delivers, or transmits ... to any foreign government, or to any faction or party or military or naval force within a foreign country, ... any document, ... [other physical items], or information relating to the national defense." To similar effect is 50 U.S.C. § 783, enacted as part of the 1950 amendments to the Espionage Act. Section 783 also prohibits the communication of classified information by an "officer or employee of the United States" to agents or representatives of foreign governments (even though such individuals were presumably already subject to liability under § 794(a)).

Finally, it is critical to note that the Espionage Act also contains two independent conspiracy provisions. Pursuant to § 793(g), "[i]f two or more persons conspire to violate any of the foregoing provisions of this section, and one or more of such persons do any act to effect the object of the conspiracy, each of the parties to such conspiracy shall be subject to the punishment provided for the offense which is the object of such conspiracy." Section 794(c) is to similar effect.

b. Espionage-Related Statutes

The Espionage Act, while important, is merely one subset of a much larger range of statutes pertaining to the unlawful disclosure of national security secrets. First, and perhaps most important, is 18 U.S.C. § 641, one of the statutes at issue (along with § 793(d) and 793(e)) in the famous case of *United States* v. *Morison*.[5] Originally enacted in 1875, § 641 applies to:

5. 844 F.2d 1057 (4th Cir. 1988).

VerDate Nov 24 2008 14:12 Feb 07, 2011 Jkt 063582 PO 00000 Frm 00069 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\63582.TXT SJUD1 PsN: CMORC

63582.042

> Whoever ... knowingly converts to his use or the use of another, or without authority, sells, conveys or disposes of any record, voucher, money, or thing of value of the United States or of any department or agency thereof ...; or
>
> Whoever receives, conceals, or retains the same with intent to convert it to his use or gain, knowing it to have been embezzled, stolen, purloined or converted ....

Thus, § 641, in general terms, prohibits the conversion of any "thing of value" to the U.S. government, and also prohibits the knowing receipt of the same, "with intent to convert it to his use or gain."

Relying on § 641, the government prosecuted Samuel Morison for transmitting photographs of a new Soviet aircraft carrier to *Jane's Defence Weekly*, an English publisher of defense information. As the Fourth Circuit explained:

> The defendant would deny the application of [§ 641] to his theft because he says that he did not steal the material "for private, covert use in illegal enterprises" but in order to give it to the press for public dissemination and information .... The mere fact that one has stolen a document in order that he may deliver it to the press, whether for money or for other personal gain, will not immunize him from responsibility for his criminal act.

Considered in conjunction with the concerns noted above, the potential liability under § 641 may be just as broad, if not broader, than the liability under §§ 793(d) and 793(e). As Judge Winter worried in *United States* v. *Truong Dinh Hung*:

> [B]ecause the statute was not drawn with the unauthorized disclosure of government information in mind, § 641 is not carefully crafted to specify exactly when disclosure of government information is illegal . . . . This ambiguity is particularly disturbing because government information forms the basis of much of the discussion of public issues and, as a result, the unclear language of the statute threatens to impinge upon rights protected by the first amendment. Under § 641 as it is written, . . . upper level government employees might use their discretion in an arbitrary fashion to prevent the disclosure of government information; and government employees, newspapers, and others could not be confident in many circumstances that the disclosure of a particular piece of government information was "authorized" within the meaning of § 641.[6]

6. 629 F.2d 908, 924–25 (4th Cir. 1980).

VerDate Nov 24 2008 14:12 Feb 07, 2011 Jkt 063582 PO 00000 Frm 00070 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\63582.TXT SJUD1 PsN: CMORC

63582.043

Also relevant to any discussion of governmental secrecy are 18 U.S.C. §§ 952 and 1924. Enacted in 1933, § 952 relates specifically to diplomatic codes and correspondence, and applies to government employees who, without authorization, publish or provide to a third-party diplomatic codes, or diplomatic correspondence "obtained while in the process of transmission between any foreign government and its diplomatic mission in the United States." A fair reading of the statute is that it prohibits the publication by the government employee, and not by an independent third-party, but the disclosure by non-governmental employees of encrypted communications between the United States and foreign governments or its overseas missions could still plausibly be said to fall within that provision's purview.

Similarly, 18 U.S.C. § 1924, enacted in 1994, prohibits the unauthorized removal and retention of classified documents or material. It applies to:

> Whoever, being an officer, employee, contractor, or consultant of the United States, and, by virtue of his office, employment, position, or contract, becomes possessed of documents or materials containing classified information of the United States, [who] knowingly removes such documents or materials without authority and with the intent to retain such documents or materials at an unauthorized location.

Three additional statutes, which regulate specific types of secret information, are also relevant to today's discussion. First among these is the Atomic Energy Act of 1954, 42 U.S.C. §§ 2011 to 2296b-7. Sections 2274, 2275, and 2277 thereof prohibit the communication, receipt, and disclosure, respectively, of "Restricted Data," which is defined as "all data concerning (1) design, manufacture, or utilization of atomic weapons; (2) the production of special nuclear material; or (3) the use of special nuclear material in the production of energy, but shall not include data declassified or removed from the Restricted Data category pursuant to section 2162 of this title." In the *Progressive* case, in which the U.S. government successfully enjoined

VerDate Nov 24 2008 14:12 Feb 07, 2011 Jkt 063582 PO 00000 Frm 00071 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\63582.TXT SJUD1 PsN: CMORC

63582.044

the publication of an article titled "The H-Bomb Secret: How We Got It, Why We're Telling It," it was the potential violation of § 2274(b) that formed the basis for the injunction.[7]

A very different statute, and one arguably of more relevance today (at least in light of the Valerie Plame affair) is the Intelligence Identities Protection Act of 1982, 50 U.S.C. §§ 421–426. Specifically, § 421 prohibits the disclosure of information relating to the identity of covert agents. Whereas § 421(a) and 421(b) prohibit the disclosure of such information by individuals authorized to have access to classified information identifying the agent, § 421(c) applies to anyone who "discloses any information that identifies an individual as a covert agent to any individual not authorized to receive classified information, knowing that the information disclosed so identifies such individual and that the United States is taking affirmative measures to conceal such individual's classified intelligence relationship to the United States." The individual must "intend[] to identify and expose covert agents and [have] reason to believe that such activities would impair or impede the foreign intelligence activities of the United States." Importantly, though, § 421(c) "does not predicate liability on either access to or publication of classified information."

Finally, the Invention Secrecy Act of 1951, 35 U.S.C. §§ 181–188, protects the disclosure of information relating to patents under "secrecy" orders. The statutory punishment, however, for disclosure of information relating to a patent under a secrecy order is forfeiture of the patent. No criminal liability appears to attach to such disclosures.

II. The Espionage Act's Key Ambiguities

For starters, it should be clear from the above survey that the Espionage Act and related statutes are difficult to parse, and often seem targeted at distinct (and perhaps

7. *See* United States v. The Progressive, Inc., 467 F. Supp. 990, 993–96 (W.D. Wis.), *appeal dismissed*, 610 F.2d 819 (7th Cir. 1979).

VerDate Nov 24 2008 14:12 Feb 07, 2011 Jkt 063582 PO 00000 Frm 00072 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\63582.TXT SJUD1 PsN: CMORC

63582.045

contradictory) goals. Although there are a number of ambiguities raised by the language of these provisions in their current form, four specific incongruities are particularly troubling.

The first—and most systematic—defect concerns the statute's ambiguous scope, by which I mean whether it applies to anything beyond classic spying. Enacted specifically to punish "espionage," which *Black's Law Dictionary* defines as "The practice of using spies to collect information about what another government or company is doing or plans to do," the plain text of the Act fails to require a specific intent either to harm the national security of the United States or to benefit a foreign power. Instead, the Act requires only that the defendant know or have "reason to believe" that the wrongfully obtained or disclosed "national defense information" is to be used to the injury of the United States, or to the advantage of any foreign nation.

As a result of this lax *mens rea* requirement, the Espionage Act could be applied as currently written to prosecute government employees or private citizens in cases bearing little resemblance to classic espionage. Such cases could include situations in which a government employee seeks to reveal the details of an unlawful secret program, or to bring to the attention of the relevant Inspector General or oversight officer the existence of information that was wrongfully classified; and cases in which a private citizen comes into the possession of classified information with no desire to harm our national security. In each of these circumstances, an informed citizen would certainly "have reason to believe" that the relevant information, if publicly disclosed, could cause injury to the national security of the United States or benefit a foreign power. That knowledge, though, need not (and often will not) bear any relationship to the defendant's actual motive.

Moreover, these concerns are hardly academic, as we've seen in the recent *AIPAC* case. There, the government prosecuted Steven Rosen and Keith Weissman, lobbyists for the

VerDate Nov 24 2008 14:12 Feb 07, 2011 Jkt 063582 PO 00000 Frm 00073 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\63582.TXT SJUD1 PsN: CMORC

63582.046

American Israel Public Affairs Committee, for receiving classified information about the Middle East, Iran, and terrorism from a Defense Department analyst before passing that information on to a journalist and an Israeli diplomat. That case involved perhaps the broadest provision of the Espionage Act, 18 U.S.C. § 793(e), which prohibits anyone in the unauthorized possession of national security information from "willfully communicat[ing], deliver[ing], transmit[ting] or caus[ing] to be communicated, delivered, or transmitted . . . [such information] to any person not entitled to receive it, or willfully retain[ing] the same and fail[ing] to deliver it to the officer or employee of the United States entitled to receive it." In upholding the first-ever use of § 793(e) in a case against non-governmental employees, the district court noted that the text of the statute "leaves open the possibility that defendants could be convicted for these acts despite some salutary motive."

The second key defect in the Espionage Act, which is related to its ambiguous scope, is the question of how, if at all, it applies to whistleblowers. For example, the Federal Whistleblower Protection Act ("WPA"), protects the public disclosure of "a violation of any law, rule, or regulation" only "if such disclosure is not specifically prohibited by law and if such information is not specifically required by Executive order to be kept secret in the interest of national defense or the conduct of foreign affairs."[8] Similar language appears in most other federal whistleblower protection statutes.

To be sure, the WPA, the Intelligence Community Whistleblower Protection Act, and the Military Whistleblower Protection Act all authorize the putative whistleblower to report to cleared government personnel in national security cases. And yet, there is no specific reference in any of these statutes to the Espionage Act, or to the very real possibility that those who receive the disclosed information, even if they are "entitled to receive it" for purposes of the

8. 5 U.S.C. § 1213(a).

VerDate Nov 24 2008 14:12 Feb 07, 2011 Jkt 063582 PO 00000 Frm 00074 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\63582.TXT SJUD1 PsN: CMORC

63582.047

Espionage Act (which itself is hardly clear), might still fall within the ambit of 18 U.S.C. § 793(d), which prohibits the willful retention of national defense information. Superficially, one easy fix to the whistleblower statutes would be amendments that made clear that the individuals to whom disclosures are supposed to made under those statutes are "entitled to receive" such information under the Espionage Act. But Congress might also consider a more general proviso exempting protected disclosures from the Espionage Act altogether.

Another important (and related) ambiguity with the Espionage Act is whether and to what extent it might apply to the press. As with the whistleblower example I just described, a reporter to whom a government employee leaks classified information could theoretically be prosecuted merely for retaining that information, and could almost certainly be prosecuted for disclosing that information (including by publishing it). And yet, it seems clear from the legislative history surrounding the Espionage Act that § 793(e) was never meant to apply to the press; indeed, as noted above, three other provisions of the Espionage Act specifically prohibit publication of national defense information, and another, broader limitation on the retention of national security information by the press was specifically scrapped by Congress, suggesting that the Act is express in those few places where it specifically targets newsgathering.

Finally, the Espionage Act is also silent as to potential defenses to prosecution. Most significantly, every court to consider the issue has rejected the availability of an "improper classification" defense—a claim by the defendant that the information he unlawfully disclosed was in fact unlawfully classified.[9] If true, of course, such a defense would presumably render the underlying disclosure legal. It's entirely understandable that the Espionage Act nowhere refers to "classification," since our modern classification regime postdates the Act by over 30

9. *See, e.g.*, United States v. Boyce, 594 F.2d 1246 (9th Cir. 1979); *see also* Scarbeck v. United States, 317 F.2d 546 (D.C. Cir. 1963).

VerDate Nov 24 2008 14:12 Feb 07, 2011 Jkt 063582 PO 00000 Frm 00075 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\63582.TXT SJUD1 PsN: CMORC

63582.048

years. Nevertheless, given the well-documented concerns today over the overclassification of sensitive governmental information, the absence of such a defense—or, more generally, of any specific reference to classification—is yet another reason why the Espionage Act's potential sweep is so broad. Even where it is objectively clear that the disclosed information was erroneously classified in the first place, the individual who discloses the information (and perhaps the individual who receives the disclosure) might still be liable.

Although statutory ambiguity is hardly a vice in the abstract, in the specific context of the Espionage Act, these ambiguities have two distinct—and contradictory—effects. Testifying before Congress in 1979, Anthony Lapham, the General Counsel of the CIA, put it this way:

> On the one hand the laws stand idle and are not enforced at least in part because their meaning is so obscure, and on the other hand it is likely that the very obscurity of these laws serves to deter perfectly legitimate expression and debate by persons who must be as unsure of their liabilities as I am unsure of their obligations.

And to whatever extent these problems have always been present, recent developments lend additional urgency to today's endeavor. In addition to the *AIPAC* case I mentioned earlier, a report released just last week by the Heritage Foundation and the National Association of Criminal Defense Lawyers (strange bedfellows, to be sure) highlighted the growing concerns among courts and commentators alike over problems of vagueness and overbreadth in contemporary federal criminal laws, let alone an antiquated statute like the Espionage Act. And just last month, the Supreme Court in the crush-video decision reiterated its concern with congressional statutes that may chill constitutionally protected speech. As Chief Justice Roberts emphasized for an 8-1 majority, the Court "would not uphold an unconstitutional statute merely because the Government promised to use it responsibly."

In short, then, although it is not my place to make specific recommendations to this Subcommittee with regard to how the Espionage Act might be updated, it seems clear that the

VerDate Nov 24 2008 14:12 Feb 07, 2011 Jkt 063582 PO 00000 Frm 00076 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\63582.TXT SJUD1 PsN: CMORC

63582.049

current state of the law is counterproductive regardless of the specific policy goals one might seek to pursue. As Judge Ellis observed in the *AIPAC* case,

> The conclusion that the statute is constitutionally permissible does not reflect a judgment about whether Congress could strike a more appropriate balance between these competing interests, or whether a more carefully drawn statute could better serve both the national security and the value of public debate. . . . [Changes in the nature of threats to our national security over the last few decades] should suggest to even the most casual observer that the time is ripe for Congress to engage in a thorough review and revision of these provisions to ensure that they reflect both these changes, and contemporary views about the appropriate balance between our nation's security and our citizens' ability to engage in public debate about the United States' conduct in the society of nations.[10]

To that end, if Congress were ultimately to conclude that the Espionage Act should be limited to cases of classic espionage and perhaps other malicious disclosures of classified information, my suggestion would be to focus carefully on the *mens rea* in the statute, and to consider the adoption of something akin to a specific intent requirement—that the offender not just know that the disclosure would be harmful to our national security, but that he or she actually intend such harm. If Congress were ultimately to conclude that the Espionage Act should instead apply to all cases of legally unauthorized disclosures of classified information, then my view is that much of the current statutory language is superfluous and unnecessary, and that a far simpler prohibition, combined with clear indicia as to the provision's scope, would avoid the myriad vagueness and overbreadth issues that currently plague the statute. If, as a third way, Congress were to conclude that there should be separate penalties for unauthorized disclosures without an intent to harm our national security, then, once more, I think more precise statutory language is called for, with clearer definitions as to the classes of individuals to which each particular provision is intended to apply.

10. United States v. Rosen, 445 F. Supp. 2d 602, 646 (E.D. Va. 2006).

VerDate Nov 24 2008 14:12 Feb 07, 2011 Jkt 063582 PO 00000 Frm 00077 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\63582.TXT SJUD1 PsN: CMORC

63582.050

Either way, though, my own view is that Judge Ellis had it exactly right that time is ripe for congressional revisiting of this statutory scheme, and I thank the Subcommittee for taking up his call.

VerDate Nov 24 2008 14:12 Feb 07, 2011 Jkt 063582 PO 00000 Frm 00078 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\63582.TXT SJUD1 PsN: CMORC

63582.051

STATEMENT OF

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

BEFORE THE

SENATE COMMITTEE ON THE JUDICIARY
SUBCOMMITTEE ON TERRORISM AND HOMELAND SECURITY

CONCERNING

THE ESPIONAGE STATUTES:
A LOOK BACK AND A LOOK FORWARD

PRESENTED ON

MAY 12, 2010

Chairman Cardin, Ranking Member Kyl and Members of the Subcommittee on Terrorism and Homeland Security, thank you for inviting me to testify before you today about the legal framework for defending our government against espionage and the disclosure of sensitive information.

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 at the Department of Justice, United States Attorney, General Counsel and Chief of Staff of the FBI and career federal prosecutor. I was honored to work with the men and women of the Intelligence Community and the many others who defend our national security apparatus against those who seek to access or disclose its most sensitive information for unauthorized purposes. I am also honored to appear today alongside my two co-panelists, both men with tremendous expertise in the field of counter-espionage.

Since the attacks of September 11, 2001, I have spent much of my professional career in the national security world, where sensitive sources and methods are the lifeblood of our national security operations. Whether it was a particular electronic surveillance we secured at the Justice Department that gave us insight into our adversaries' terrorist plans or source information that factored into decision making at the White House, I have seen the vital role that sensitive information plays in our national security operations and how those operations can be put in jeopardy whenever that information is compromised. And unfortunately, that information is compromised all too frequently.

While every disclosure of sensitive information is different in terms of motive and parties, for purposes of this discussion I would like to focus on two general categories. The first category includes those instances where a government official passes sensitive information to an agent of a foreign government or other foreign power -- the classic espionage scenario with spies like Aldrich Ames or Robert Hanssen who betray their country for money, out of resentment against their government or agency, or out of misplaced loyalty or affinity for another country or foreign power. The second, and more common, scenario is the leak of sensitive information to the press by a government official whose motive may range from base self-interest to a laudable whistleblower's desire to change government operations for the better.

We are all quick to condemn the traitorous actions of the classic spies, and the Justice Department has mounted strong prosecution efforts whenever such spies have been identified over the years. We must also recognize, however, that the media leaker can do grievous damage to our national security.

While I appreciate that some of those responsible for media leaks -- i.e. the "whistleblowers" -- may genuinely feel they are acting in the country's best interests, I share the concern expressed by many in Congress about the need to enhance our defenses against such disclosures. An important part of that effort is ensuring that, in the

63582.053

appropriate cases, we investigate and prosecute those who disclose our operational secrets. As you know, however, the Department of Justice does not have a lengthy record of successful leak prosecutions. While it has brought many strong espionage cases over the years, there have been very few prosecutions for leaks to the media.

That thin track record is not for a lack of effort on the part of the investigators and prosecutors. Rather, it is a result of the myriad obstacles that stand in the way of building a prosecutable media leak case. Those obstacles are many, and they include the following:

First, it is often very difficult to identify the leaker in the first place, given the large universe of people who often are privy to the sensitive information that was disclosed. It is not uncommon for many people to be read into the most highly-classified program or to be recipients of intelligence derived therefrom -- a problem which has only gotten worse with the increased integration and information-sharing we have seen in the intelligence and law enforcement communities since the 9/11 attacks.

Second, our leak investigations operate under the limitations in the Justice Department's internal regulations, which make it difficult to obtain information from the one party who is in the best position to identify the leaker -- the member of the media who received the leaked information. These regulations have been in place for years, and they serve the important purpose of ensuring that "the prosecutorial power of the Government [is] not . . . used in such a way that it impairs a reporter's responsibility to cover as broadly as possible controversial public issues." United States Attorneys' Manual, Section 9-13.400. The upshot is, however, that an investigator who wants to use a subpoena to compel information from a reporter can do so only after the Attorney General personally grants his or her permission -- a process that has resulted in only about two dozen subpoenas to the press over the past couple decades.

Third, even when the leaker is identified, the agency whose information was compromised is often reluctant to proceed with the prosecution. The concern is that charging and trying the case will both highlight the compromised information and likely result in the disclosure of further sensitive information that may come within the ambit of criminal discovery or admissible evidence. While the Classified Information Procedures Act helps to minimize the effects of the latter, there is always a concern about disclosure when a national security crime is prosecuted and brought to a public trial.

Finally, even if the Justice Department succeeds in identifying and indicting the suspected leaker, it can expect to face a vigorous defense. These cases typically feature legal challenges from defense counsel invoking everything from first amendment principles to allegations of improper classification to arguments that their client's alleged leak was actually an authorized disclosure within the scope of his or her official duties. The Rosen and Weissman case that was recently dismissed after years of litigation is an example of the difficult issues that these cases present.

63582.054

For all these reasons, leak cases are exceptionally challenging, and successful prosecutions are few and far between.

The question for today is whether any of these obstacles can or should be addressed by changes to the governing legislation. While I agree with those who find the espionage statutes cumbersome and antiquated in their approach and terminology, I do not see a legislative silver bullet that would overcome all of these obstacles.

There are, however, a few areas of legislative initiative this Committee might wish to consider.

First, the committee might examine whether government contractors are adequately covered by the espionage laws. These statutes were drafted before the influx of contractors into the government's most sensitive operations. The past few decades have seen a dramatic increase in the number of private contractors who carry the highest clearances and share in the government's most closely-guarded secrets. While prosecutors can reach private contractors with most of the provisions in the espionage statutes, there is one important provision prohibiting the disclosure of classified information by a government official to a foreign power -- 50 U.S.C. Section 783 -- which does not extend to contractors. While prosecutors may still succeed in developing a case based on other statutes -- which, unlike Section 783, are not limited to government employees -- there are scenarios where a contractor's espionage would be more difficult to prosecute because of that gap in the statute. In the absence of any principled reason for treating them differently, Congress could consider putting government employees and contractors on the same footing in that provision.

Second, Congress could consider amending the Classified Information Procedures Act to ensure better protection of sensitive information in criminal trials. Experience with that statute since 9/11 has pointed up a number of areas where CIPA could do a better job of accommodating the government's concerns about classified information in public criminal proceedings. As Senator Kyl has proposed, the statute can be improved by: (1) mandating that the government can submit its arguments for protecting classified information in the discovery process directly to the court without having to share those arguments and the classified information with the defendant; and (2) clarifying that the government can appeal any trial judge's ruling that runs the risk of causing classified information to be disclosed at trial. Others have suggested different amendments, such as clearly authorizing courts to keep the public from seeing sensitive information being used at trial -- an issue that was vigorously litigated in the Rosen and Weissman case -- or explicitly allowing for anonymous testimony by intelligence officials operating under cover. With the current national discussion about prosecuting more international terrorism cases in Article III courts, this would be a good time to consider these and other suggestions for amending CIPA and enhancing our ability to protect sensitive information that is used in the criminal process.

Third, Congress might consider providing a definition of protected "defense information" that fully covers the foreign affairs information -- such as information about

63582.055

other governments' personnel, plans and policies -- that is so vital to formulating our foreign policy and calibrating our posture vis-à-vis other countries.

In a more general sense, Congress can use this hearing -- and any ensuing hearings -- to encourage respect for our nation's operational secrets. Congress can send the basic message that it does not condone the unauthorized release of classified information about our national security operations. It can point out, for instance, that whistleblowing is no longer a sufficient justification for divulging secrets. In the situation where a well-meaning government official sincerely feels the need to "blow the whistle" on perceived government misconduct, there are now lawful channels for doing so. Congress has passed whistleblower statutes that facilitate and protect genuine whistleblowing, including the Intelligence Community Whistleblower Protection Act, which provides a procedure for whistleblowers to advise the Intelligence Committees about alleged wrongdoing in an intelligence program without publicly disclosing sensitive information about that program.

Congress can also encourage the Administration in its efforts to staunch the outflow of sensitive information by pursuing investigations into those leaks that are particularly egregious or damaging.

Finally, Congress can encourage the intelligence agencies in their effort to use administrative sanctions to deter leaking within their ranks. Recognizing the difficulties of using the criminal process -- even when the leaker can be identified -- agencies have instead focused on sanctioning the responsible employee with personnel action or withdrawal of his or her security clearances. Although they do not pack the punch of a criminal conviction, such sanctions nonetheless have a significant deterrent effect on the rest of the workforce.

* * * * * * * *

No matter where one stands on the political spectrum or in the current national security policy debates, we should all recognize that the unchecked leaking of sensitive information can cause grave harm to our national security. Congress plays an important role in addressing that problem -- whether by legislation, by oversight or by simple exhortation -- and I applaud this Committee for the initiative it is showing with today's hearing.

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

○

63582.056