

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

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.

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 about 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

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

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.

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

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

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

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.

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.

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.

- 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

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.