

**STATEMENT OF**

**KENNETH L. WAINSTEIN  
PARTNER, CADWALADER, WICKERSHAM & TAFT LLP**

**BEFORE THE**

**SUBCOMMITTEE ON CRIME, TERRORISM  
AND HOMELAND SECURITY  
COMMITTEE ON THE JUDICIARY  
HOUSE OF REPRESENTATIVES**

**CONCERNING**

**NATIONAL SECURITY LEAKS**

**PRESENTED ON**

**JULY 11, 2012**

Chairman Sensenbrenner, Ranking Member Scott and distinguished Members of the Subcommittee, thank you for inviting me to testify before you today about the issue of national security leaks.

My name is Ken Wainstein, and I am a partner at the law firm of Cadwalader, Wickersham & Taft. Prior to my leaving the government in January of 2009, I was honored to work for many years with the men and women of the Intelligence Community and others who defend our national security against our adversaries. I am also honored to appear today alongside my co-panelists, who bring a wealth of experience to a discussion of this critically important issue.

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 source information that factored into decision making at the White House or intelligence from a wiretap we secured at the Justice Department, 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.

The problem of national security leaking has come to the fore recently because of several particularly damaging leaks over the past few months. While these leaks are alarming, they are sadly only the most recent manifestations of an age-old problem. The reality is that government leaking has been happening for as long as there has been government, and every American administration since the founding of the Republic has suffered its share of leaks.

While some leaks may be innocuous or simply embarrassing, others can be severely damaging to our national security. Leaks of national security information can compromise all aspects of our national security program, including:

- National security operations: From the 1942 newspaper report that the U.S. had broken the Japanese military code to the 2006 disclosure of the Treasury Department's secret program for tracking terrorist finances, we have repeatedly seen vital operations put in jeopardy by careless or malicious leaks.
- Human sources: A key element of any intelligence program is the source -- the human being who is positioned to provide intelligence on an adversary and its plans and intentions. Whenever a source's identity is leaked from the government -- as apparently happened when it was reported that a Saudi source had played a central role in the foiling of Al Qaeda's recent airplane-bombing plot -- it not only negates the effectiveness of that source; it also undermines our ability to develop other sources.
- Methods: Leaks about our methods tip our hand to our adversaries and give them the opportunity to adapt their defenses against those methods. A classic example

is the recent disclosure of our alleged use of malware to attack the Iranian nuclear weapons program.

- Government personnel: Obviously, leaks can also prove dangerous or fatal to our personnel in sensitive positions, as was tragically demonstrated by the murder of the CIA's Chief of Station in Athens by terrorists in the 1970's after his outing by a former CIA employee.
- Alliances: Leaks from within our government can undermine those relationships with foreign services that are so vital to our national security, especially in relation to our effort against international terrorists.
- The integrity of government service: Finally, it's worth noting that government employees with clearances give a personal promise that they will protect the government's classified information. The integrity of public service is diminished whenever that promise is broken.

In assessing why leaks happen and what should be done to prevent them, we have to examine the reasons why people leak in the first place. While there are a range of motives behind different leaks and leakers, I will put those motives into two general categories for discussion. The first category includes those instances where a government official passes sensitive information to 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. We all condemn the traitorous actions of these classic spies, and the Justice Department has mounted strong prosecution efforts whenever such spies have been identified over the years.

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. 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 appropriate cases, we investigate and prosecute those who disclose our operational secrets.

As you know, however, the Justice Department 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 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, 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 serve as a procedural bulwark protecting the vital role of the free press in our democracy. These regulations ensure 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 or three dozen subpoenas to the press for source information 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 address this problem, 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 dismissed after years of litigation is an example of the difficult issues that these cases present.

For all these reasons, leak cases are exceptionally challenging, and successful prosecutions are few and far between. The question for Congress is whether any of these obstacles can or should be addressed by changes to the governing legislation. I agree with those who find the current espionage statutes cumbersome and antiquated in their approach and terminology, and I would support Congress' effort to reform them.

This reform effort will be complicated, and will entail some very carefully calibrated lawmaking. Because it directly implicates the tension between national security and our First Amendment values, legislating in this area is challenging and raises a host of complex issues. For example, consideration of a law that flatly prohibits and

punishes any disclosure of classified information will require examination of the problem of over-classification of government information. Similarly, the strengthening of legislation targeting government leakers may require an examination of the whistleblower protection acts to ensure that true whistleblowers can get their concerns raised and addressed without going to the press. Finally, any effort to revise the Espionage Act will lead to a debate whether the person who receives and publishes leaked information (i.e. the press) should be subject to the same criminal exposure as the government employee who committed the leak.

These are certainly complex issues, and they will require careful consideration. Given the damage caused by the continued leaks and the inadequacy of our current leak legislation, however, it is important that Congress take these issues on and consider an appropriate legislative response.

\* \* \* \* \*

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, 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 questions you may have.