Testimony of
Kate Martin, Director
Center for National Security Studies

Before the
Committee on the Judiciary
United States House of Representatives

"Oversight of the Administration's use of FISA Authorities"
Wednesday, July 17, 2013

Chairman Goodlatte, Ranking Member Conyers, and distinguished Members of the House Judiciary Committee, thank you for inviting me to testify today. I am the Director of the Center for National Security Studies a think tank and civil liberties organization, which for almost 40 years has worked to ensure that civil liberties and human rights are not eroded in the name of national security. The Center is guided by the conviction that our national security must and can be protected without undermining the fundamental rights of individuals guaranteed by the Bill of Rights and that respect for our constitutional system of government will accomplish that. In our work on matters ranging from national security surveillance to intelligence oversight, we begin with the premise that both national security interests and civil liberties protections must be taken seriously and that by doing so, solutions to apparent conflicts can often be found without compromising either.

I appreciate the Committee's long history of work since 9/11 on the amendments to the Foreign Intelligence Surveillance Act (FISA) contained in the Patriot Act and the many amendments since then, including the 2008 Foreign Intelligence Amendments Act, and its serious consideration of the civil liberties concerns expressed by my organization and our colleagues.

I want to raise two overarching concerns for this Committee's consideration during the current debate, which I hope will inform your consideration of necessary oversight measures as well as specific changes to the statutory language. First, we are concerned that the unprecedented massive collection of information on Americans, the creation of secret databanks which are available for government analysis, queries, and data-mining by ever increasingly sophisticated computerized tools, and the dissemination of both raw information and the results of such analysis or data-mining throughout the executive branch pose unprecedented threats to First and Fourth Amendment liberties. Second, the secrecy that surrounds this government surveillance – not of foreign governments or other foreign targets – but of Americans – poses a significant and perhaps unprecedented challenge to our system of constitutional checks and balances.

It has long been recognized as Senator Sam Ervin, the author of the Privacy Act put it in 1974:

> *"[D]espite our reverence for the constitutional principles of limited Government and freedom of the individual, Government is in danger of tilting the scales against those concepts by means of its information gathering tactics and its technical capacity to store and distribute information. When this quite natural tendency of Government to acquire and keep and share information about citizens is enhanced by computer technology and when it is subjected to the unrestrained motives of countless political administrators, the resulting threat to individual privacy makes it necessary for Congress to reaffirm the principle of limited, responsive Government on behalf of freedom.*
>
> *Each time we give up a bit of information about ourselves to the Government, we give up some of our freedom: the more the Government or any institution knows about us, the more power it has over us. When the Government knows all of our secrets, we stand naked before official power. Stripped of our privacy, we lose our rights and privileges. The Bill of Rights then becomes just so many words."*

Senator Sam Ervin, June 11, 1974, reprinted in Committee On Government Operations, United States Senate And The Committee On Government Operations, House Of Representatives, Legislative History Of The Privacy Act Of 1974, S.3418, at 157 (Public Law 93-579)(Sept. 1976).

A key purpose of the Fourth Amendment was to prevent general searches by the government. This was accomplished in part through the Amendment's requirement of particularity -- that the target of a search or seizure, the place to be searched, the things to be seized all had to be specifically identified in a warrant issued by a judge. We now face the situation where the government has the capacity to collect massive amounts of information on millions of Americans, to store that information indefinitely, and to analyze that information to discover enormous amounts of revealing information about individual Americans' private lives and political activities. As others have demonstrated, the underlying rationales for the old distinctions between content and meta-data, or the notion that Fourth Amendment protections have no applicability to information about an individual held by third parties, no longer hold in the new world of massive electronic data about individuals held by Internet service providers, telecommunications companies and others.

At the same time, there has been a fundamental shift in the way that the government collects information on Americans. The two sections of FISA that have been the focus of the leaks, 50 U.S.C. § 1861, 1881a , "sections 215 and 702", are apparently used by the government to obtain information about thousands of communications of Americans, but without even any suspicion about the individual Americans whose communications are being collected. To the contrary, these authorities are apparently being used for en masse bulk collection on thousands or

millions of individuals without any individualized showing of suspicion about any party to the communication, whether American or foreigner. While it is true that the NSA has had such bulk collection capabilities for many years, those capabilities were aimed overseas and their purpose was to collect information about foreign governments and foreign terrorist organizations. That collection did include "incidentally acquired" information on Americans' communications, but that was not the purpose of the collection, and there were strict rules about the NSA disseminating that information to other government agencies for their use. Nor, as far as we know, was the government creating massive databases on Americans' communications as an integral part of its "foreign intelligence" activities.

Questions about these FISA authorities:

As others have detailed, there are serious questions whether these bulk collection programs are within the intended statutory authorizations, e.g., the domestic telephony meta-data program under sec. 215. There are serious constitutional concerns about the breadth of and lack of individualized suspicion or particularity in these programs. And there are serious questions whether the secrecy built into the programs is constitutional and whether it is consistent with effective oversight or a working system of checks and balances.

In examining these authorities and programs, it is important to review not only whether private information about Americans held in government databases is adequately protected from rogue employees or contractors stealing or misusing the information. While safeguards are needed against that kind of privacy abuse, the more important danger is that there are inadequate safeguards against government violations of the law or against deliberate misuse of the information to target the government's political opponents, chill dissent or unconstitutionally profile minority communities. As the original Framers recognized, all governments may succumb to the temptations of power. In my lifetime Senator McCarthy smeared civil servants, the FBI tried to blackmail Dr. Martin Luther King in order to weaken the civil rights movement, President Nixon created an enemies list of his political opponents, and the Justice Department wrote a secret legal opinion that the President could break the law in secret if he deemed it necessary for national security.

Since the leaks about these two particular programs, the Executive Branch has vigorously defended their usefulness in detecting and stopping terrorist plots and that is certainly relevant to the Congress' and public consideration. These claims merit careful analysis, especially in light of former NSA Director Michael Hayden's explanation that it is very difficult to determine which information was key in stopping any particular attack.[1] And in doing that analysis, there are at least two key questions to be considered: are there less intrusive ways to obtain this

[1] "…you know – we're asking for evidence that A caused B. And right now, if we're really good at our art, you'll never be able to do that. It'll all be a blend of different pieces of glass that you now get to create a mosaic from." Remarks of General Michael Hayden, "Is Big Brother Watching You?" American Enterprise Institute, June 19, 2013, http://www.aei.org/events/2013/06/19/is-big-brother-watching-you/.

information and more importantly, are there other equally or more effective counter-terrorism measures available. We have already begun to see alarmist statements unsupported by any analysis to the effect that without these programs, we face another 9/11. Such statements interfere with, rather than serve a careful and deliberate consideration of the issues.

The dangers of secrecy:

In addition to the fundamental change in the scope of and authority for government surveillance of Americans, the attendant secrecy has made it almost impossible to have the kind of informed public debate and democratic decision-making fundamental to the notion of self-government. It is not debatable that secrecy increases the danger that government will overreach. At the same time, there is no question that foreign intelligence activities depend to some degree on secrecy. A democracy must continually work to figure out ways to provide for the national defense while respecting civil liberties and preserving constitutional government. The increase in technological surveillance capabilities, global connectedness and the reliance on electronic communications has made doing this more complex.

The expansion of secret government surveillance and secret legal authorities especially in the last 12 years requires us to ask whether we are witnessing the serious erosion of our constitutional system of checks and balances and the rise of a system of secret law decreed by courts, carried out in secret, enabling the creation of massive secret government databases on Americans' personal and political lives. As you know, the system of checks and balances relies upon the existence of a Congress which engages in a public debate informed by the relevant information from the Executive; courts which hear two sides argue a question and know their opinions are subject to appeal and public critique; and an Executive branch who will be called to account for ignoring the law. All of this in turn depends upon an engaged press and informed public.

First step: necessary public disclosures:

The President has declared that he welcomes this debate and the Administration has already declassified some important information. This hearing and this Committee's involvement in the debate is a crucial step in restoring the needed transparency. The fact that the NSA is involved and that these programs (or at least the 702 program) may include legitimate foreign intelligence activities that do not affect Americans should not be used as a reason to bypass the jurisdiction of this Committee or the Senate Judiciary Committee. As this Committee has recognized ever since the introduction of the Patriot Act, surveillance authorities concerning information on Americans is at the core of this Committee's responsibilities; and congressional and executive branch procedures and rules for considering such legal authorities and conducting oversight should recognize the Judiciary Committees as full partners with the Intelligence Committees in these activities. As long ago as 1990, the Justice Department expressed concern

about the involvement of the Judiciary Committees.[2] This concern is not only misplaced, but inappropriate and we urge you to call upon the Executive Branch to treat the Committee as a full partner going forward and to insist that the rules of the House implement that understanding.

We urge the Committee first to insist on disclosure of sufficient information to enable the public to understand the existing legal authorities for national security surveillance of Americans and the scope of such surveillance. Such disclosures are necessary for an informed public debate, which in turn can inform Congress' consideration of these issues. We appreciate the legislation offered by the Ranking Member and others to accomplish this. However, we do not believe that legislation should be required in order to obtain the necessary disclosures from the Executive Branch and urge the Committee to make clear to the Executive Branch that you expect the necessary information to be disclosed as soon as possible and without waiting for enactment of legislation.

That information should include a full explanation of the FISA court's interpretations of existing law and the Executive's legal arguments made to the court, whether or not the court accepted them. If redaction of the court opinions and government pleadings is too time-consuming or difficult, the Executive should prepare a White Paper as soon as possible as it did in January 2006 about its legal basis for the NSA warrantless program after that program was revealed by The New York Times in December, 2005.

It is also essential to disclose the scope of the programs' collection and retention of information on Americans. As Professor Daniel Solove has pointed out: "secrecy at the level of

[2] In 1990, DOJ's Office of Intelligence Policy and Review wrote a memo to the Office of the Deputy Attorney General explaining that it had been "working with the National Security Agency for the past three years to develop possible amendments to the Foreign Intelligence Surveillance Act to meet a need created by technological advances." … The 1990 memo … identified several "policy and tactical issues" counseling against seeking new legislation. David S. Kris, "Modernizing the Foreign Intelligence Surveillance Act: Progress To Date and Work Still to Come," in *Legislating the War on Terror, An Agenda for Reform,* Ed. Benjamin Wittes, Georgetown University Law Center and The Brookings Institution, 217-251 (2009). These "policy and tactical" issues, included: "the fact that "committee jurisdiction in both the House and Senate is concurrent between the Intelligence and Judiciary Committees," and while the "problems giving rise to the possible amendments have all been discussed with the Intelligence Committees," they had not been discussed "with the Judiciary Committees"; "the risk of added congressional restrictions if the statute is opened up to amendment"; and " the fact that "the proposed amendment to FISA to resolve the NSA problem . . . *is certain to be written in such enigmatic terms that only those who have been briefed in executive session will understand them," thus risking "speculation in the media about what is really intended and probably deep suspicion that something sinister is going on*" (emphasis added). "Thoughts on a Blue-Sky Overhaul of Surveillance Laws: Challenges," by David S. Kris, *Lawfare,* May 19, 2013, http://www.lawfareblog.com/2013/05/thoughts-on-a-blue-sky-overhaul-of-surveillance-laws-challenges/#fn1. It is not clear that the Justice Department yet understands that the only antidote to media speculation and deep suspicion by the American public is openness about what is going on.

an individual suspect is different from keeping the very existence of massive surveillance programs secret." "Five myths about privacy," Daniel J. Solove, *The Washington Post*, June 13, 2013, http://www.washingtonpost.com/opinions/five-myths-about-privacy/2013/06/13/098a5b5c-d370-11e2-b05f-3ea3f0e7bb5a_story.html. Keeping secret the identification of any particular individual or group subjected to surveillance may be necessary in order to effectuate the goals of the surveillance, at least for so long as the surveillance and the underlying investigation continues. But to the extent that disclosure of the scope of U.S. government collection programs on Americans may make some investigations somewhat harder – and counterterrorism experts dispute that[3] – there is an overriding interest in public disclosure because it is essential to a democratic debate and decision on what is the proper scope of these programs. (Furthermore the rationale for keeping secret the legal interpretation of section 215 -- that disclosing the government's claim that legal authority exists for such a program, would reveal the existence of the program and thereby render it useless -- seems to have been undercut by the government's claim that the program continues to be necessary, even though its existence is now public.)

Public explanation and disclosure of related surveillance authorities, not just the 215 and 702 programs is also essential.

- For example, the press reports that there was a similar program to collect internet metadata that was halted in 2011. This Committee should insist that the Executive Branch publicly disclose whether such a program existed, what legal authorities were used; whether in its view existing legal authorities would allow the resumption of such program, and whether the government still maintains the metadata collected by that program.

- This Committee should demand public disclosure from the Executive Branch concerning whether section 215 or any other authority would allow mass collection of other kinds of records held by third parties, e.g., medical records, credit card records, or financial records. If not, then the Executive Branch should disclose why not.

- This Committee should also demand disclosure of any other FISA court opinions (or summaries) concerning legal authority for surveillance of Americans. The existence of such an opinion in 2007 has been hypothesized: "As far as I can determine, the government seems to have persuaded the FISA Court in January 2007 that the international gateway switches, which essentially are the junctions between the U.S.

[3] "The argument that this sweeping search must be kept secret from the terrorists is laughable. Terrorists already assume this sort of thing is being done. Only law-abiding American citizens were blissfully ignorant of what their government was doing." "Why you should worry about the NSA," Richard A. Clarke, *New York Daily News*, June 12, 2013, http://www.nydailynews.com/opinion/worry-nsa-article-1.1369705#ixzz2Z8OKOmUm.

and the rest of the world's telecommunications grids, are reasonably particular FISA "facilities," and that al Qaeda is using them. If that is right, it means that a handful of orders gave the government access to all, or almost all, of the international telecommunications traffic entering or leaving the United States. That is very speedy and agile. . . . The problem, of course, is that while al Qaeda is using those switches, so is everyone else. Even under the most extreme estimates, al Qaeda cannot account for more than a tiny percentage of calls transiting the switches." David Kris, "A Guide to the New FISA Bill, Part II," *Balkinization*, June 22, 2008, http://balkin.blogspot.com/2008/06/guide-to-new-fisa-bill-part-ii.html.

- The scope of existing legal authorities can only be understood by understanding the history of FISA court opinions, even if such a 2007 opinion has been superseded by the 2008 enactment of the FISA Amendments Act.

- This Committee should demand public disclosure from the Executive Branch of a complete report concerning the overlapping authorities for collection of information about Americans' communications, e.g., national security letter authorities; pen register/trap and trace authorities. Without an understanding of how these authorities overlap and differ, it will be difficult to legislate adequate protections for privacy and First Amendment rights.

- This Committee should demand a complete public report from the Executive Branch concerning what rules apply to accessing, analyzing, data-mining, keeping, using or disseminating information concerning Americans' communications. That includes not only the "minimization rules" which have been classified without any apparent necessity for doing so, but rules and regulations issued by different agencies, for example, the FBI and DoD. As a former official and recognized expert in the field explains: "Today, a good deal of foreign intelligence collection is regulated by the Fourth Amendment and Executive Order 12333 and its subordinate procedures, *but not in any meaningful way by statute (emphasis added).*" David Kris, "Thoughts on a Blue-Sky Overhaul of Surveillance Laws: Approach," *Lawfare*, May 20, 2013, http://www.lawfareblog.com/2013/05/thoughts-on-a-blue-sky-overhaul-of-surveillance-laws-approach/.

The number, complexity and overlap of authorities and rules is such, that a simple list of them will not be sufficient for the public to understand what its government is up to, nor for the Congress to exercise meaningful oversight. The Executive Branch, however is operating on the basis of an understanding concerning the standards and scope of legal collection and use of information about Americans. That understanding needs to be publicly shared with the Congress and the American public.

Substantive fixes to limit massive government surveillance and provide safeguards:

The current controversy provides an important opportunity to reexamine the existing surveillance regime. That examination depends upon a public accounting of what the government is doing, in order to have a debate regarding its risks and benefits and possible alternatives.

In order to ensure that such an accounting happens, we urge the Committee to consider revisiting the existing sunset for the FISA Amendments Act and to shorten it to align with the existing sunset for section 215 in mid-2015, so that these authorities will be revisited together. While there are some immediate fixes that could be adopted, it is crucial not to overlook the more fundamental questions at stake. For example, proposals to require more transparency of FISA court opinions or some kind of court advocate to oppose the government in secret , while perhaps useful, are not sufficient to address the fundamental change in judicial function wrought by giving the FISA court the job of approving programmatic surveillance or making constitutional rulings in situations where the individual whose rights are at stake not only never has an opportunity to appear before a court and challenge the ruling, but is never even informed that the government has amassed information about her.

There are also significant and complex technical questions that should be understood in evaluating these programs and designing safeguards, which questions have not yet been adequately discussed or analyzed. See for example Remarks of Steven M. Bellovin and Daniel Weitzner before the Privacy and Civil Liberties Oversight Board, July 9, 2013, http://www.pclob.gov/9-July-2013. A former NSA mathematician and analyst has also proposed a way whereby when the NSA collects and analyzes massive amounts of data on Americans without any particularized warrant, a warrant would be required before the identity of that American and the results of that analysis or information could be shared with other parts of the government and acted upon.[4]

Again, we appreciate the opportunity to appear before the Committee as part of this work and would be pleased to offer whatever further assistance might be useful.

[4] See William Binney's description in "The Secret Sharer, Is Thomas Drake an Enemy of the State?" Jane Mayer, *The New Yorker*, May 23, 2011, http://www.newyorker.com/reporting/2011/05/23/110523fa_fact_mayer?currentPage=all.