LECTURE ON NSA AT DARTMOUTH NOVEMBER 14, 2013

(Slide 1)

Before I start my presentation I want to tell a story, a story that is directly related to today's theme.

My wife Lois and I were recently driving around the back roads of Vermont and saw a sign in front of a well-worn log cabin obviously "off the grid".

The sign caught my eye not just because it was painted on an old piece of plywood, but also especially because it said "Talking Dog for Sale". Who could pass up the opportunity to see what story might lie behind that sign.

I pulled into the driveway behind a rusted-out Chevy pick-up and tooted the horn. A heavily bearded old gent, as well-worn as his cabin, appeared and assured me he did indeed have a talking dog in the back yard and took us back to see him. To my surprise there was a decently groomed and intelligent looking Labrador retriever sitting there.

I understand you can talk, I said.

***"Yep"*, the Lab responded.**

After I recovered from the shock of hearing a dog talk, I asked 'So, what's your story?'

The Lab looked up and said, *"Well, I discovered that I could talk when I was pretty young. I wanted to help my country, so I went to the NSA who I heard needed good listeners who could keep their mouths shut and told them I was available".*

"In no time at all they had me jetting from country to country, sitting in rooms with diplomats, generals, and terrorists because no one figured a dog would be eavesdropping and could tell what he heard. Bin Laden liked to pet me but his treats were terrible. Little did he know that a dog is not always a man's best friend.

"I was one of their most valuable spies for eight years running."

"But the jetting around really tired me out, and I knew I wasn't getting any younger so I decided to settle down. I signed up for a job at the Burlington airport to do some undercover security, wandering near suspicious characters and listening in."

"I uncovered some incredible dealings and was awarded a batch of medals."

"Finally I retired, got married, had a mess of puppies, and now I'm just spending time with my family."

I was amazed; especially since this was an NSA secret I had never been told.

I turned to the old gent and asked how much he wanted for the dog.

***"Ten dollars,"* he said.**

Ten dollars?

This dog is incredible and you only want ten dollars for him?

Why on earth are you selling him so cheap?'

"Because it's all lies.

He's never been out of the yard."
(Slide 2)

Well, I have been out of the yard and I am going to do my best to give you my honest view of how you have been given a very distorted and untrue view of one of our most productive intelligence agencies that targets foreign terrorists and not its own citizens.

That distorted view has come from the thousands of NSA documents stolen by Edward Snowden and sent to the Washington Post, the New York Times, The Guardian, and perhaps Der Spiegel. Their reporters have all too frequently not understood what they were looking at and have sensationalized all that they could. Especially as it relates to their

claims that NSA is targeting US persons. Which NSA does not do, as we shall examine in this presentation today.

My talk will be based not only on my own experience with NSA and the law, but more importantly on recently declassified documents of the Foreign Intelligence Surveillance Court, the Department of Justice, the Director of National Intelligence and the Director of the National Security Agency.

You can view all the declassified documents by going to www.dni.gov.

(Slide 3)

The debriefing document I signed with NSA when I moved to the Upper Valley and stopped consulting in 2004 does not permit me to discuss any matters that are still classified. And there is no point in your going to look for the dog because he can't talk either.

I will try to leave ample time for Q & A at the end.

(Slide 4)

I. CREATION AND MISSION OF NSA

President Harry Truman created the National Security Agency in a memorandum of November 4, 1952, entitled "Communications Intelligence Activities".

The Truman Memo established NSA as an element of the Department of Defense to unify under a single military director the squabbling, competing, and uncoordinated activities of the three service signals intelligence elements – the Army Security Agency, the Air Force Security Service and the Naval Security Group.

Although NSA was established in the Department of Defense, it was established as a national foreign intelligence agency to "satisfy the legitimate [foreign] intelligence requirements" of all executive departments and agencies of the US government.

NSA was given a very specific foreign intelligence mission – "to provide an effective, unified organization and control of the communications intelligence activities of the United States conducted against foreign governments and to

provide for integrated operational policies and procedures pertaining thereto".

(Slide 5)

What is meant by "communications intelligence activities"? Very simply, communications intelligence is the substantive part of signals intelligence which entails the interception and acquisition of foreign electronic transmissions of whatever type – voice, computer, email, facsimile, radar, telemetry, plain text or encrypted that will be responsive to the documented information needs of the US government.

(Slide 6)

NSA does not decide what foreign information it will try to collect. A national process called the National Intelligence Priorities Framework managed by the Director of National Intelligence for the President and the National Security Council determines that. The President and the NSC Principals Committee twice yearly provide the DNI with their statement of foreign intelligence topics and priorities that he must task to all the elements of the intelligence community.

NSA's mission is to try to satisfy those foreign intelligence requirements through the acquisition of foreign communications used by foreign powers and institutions, military forces, intelligence and espionage organizations, purveyors of weapons of mass destruction and especially since 9/11, terrorist organizations.

I have deliberately used the word "foreign" ten times thus far.

In spite of what the media apparently would like its readers to believe, NSA's mission is foreign intelligence, not domestic. NSA has neither the authority nor the responsibility to intercept domestic communications exclusively between US citizens and persons. In fact it is strictly illegal for it to do so. Neither NSA nor any other element of the Intelligence Community - except the FBI – may undertake any foreign intelligence collection for the purpose of acquiring information concerning the domestic activities of US persons.

II. US Intelligence and the Law (Slide 7)

The laws and directives controlling US intelligence activities are exhaustive and clear.

The public in general and perhaps many of you in this room perceive US intelligence agencies as lacking in accountability and, as these agencies operate in secrecy, totally uncontrolled. That certainly appears to be the perception of the media where you get most of your information, especially as related to the current reporting on NSA.

The facts of the matter are totally different. We do not have the time today to delve in detail into all the laws, executive orders and regulations controlling the missions and actions of all these agencies but I urge you to do some research on your own so you are better prepared to critically examine what the media presents to you. Three readably available sources of these laws are:

(Slide 8)

(1) ***The Intelligence Community Legal Reference Book*** **(941 pages) found at www.dni.gov/files/documents/IC_Legal_ref_2012.pdf;**

(2) U.S. Intelligence Community Law Sourcebook: A Compendium of National Security Related Laws and Policy Documents, **published by the Standing Committee**

on Law and National Security of the American Bar Association (2010);

(3) CRS Report for Congress - Privacy: ***An Overview of Federal Statutes***

Governing Wiretapping and Electronic Eavesdropping (October 9, 2012)

III. The Law and NSA

A. **Fourth Amendment - Search and Seizure - (Slide 9)**

The starting point for laws controlling NSA's signals intelligence mission to ensure the agency does not spy on US persons is the Constitution itself, namely the 4th Amendment.

> ***The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.***

The message of the 4th Amendment is clear and its application to private and personal electronic communications, papers, and documents has been made part of our legal framework. In my former organization at NSA I insisted that all the analysts working for me were fully briefed on the 4th amendment by our lawyers and that the analysts understood its controlling relevance to the follow-on laws and directives I will now cover.

B. Executive Order 12333 – (Slide 10)

The President of the United States manages the operations of the Executive branch of Government through Executive orders. Presidential executive orders are considered to have the force and effect of law as they are founded on the authority of the President derived from the Constitution.

Executive Order 12333, issued by President Reagan in 1981, sets forth the duties and responsibilities of US intelligence agencies as well as placing numerous and specific restrictions on their activities.

The Executive Order's purpose is to establish an intelligence system to satisfy the need for timely, accurate, and insightful information about the activities, capabilities, plans, and intentions of foreign powers, organizations, and persons, and their agents, as well as the detection and countering of international terrorist activities, the spread of weapons of mass destruction and espionage.

While Executive Order12333, amended by each subsequent President, remains the present and most comprehensive statement of US intelligence activities, it was modeled on previous orders issued by Presidents Ford and Carter. Ford's Executive Order 11905, issued in 1975, was the first official comprehensive public description of all the US intelligence agencies and their missions. It specified their responsibilities, the authorities under which they operated, and the restrictions placed upon them.

(Slide 11)

NSA's mission, as spelled out in EO 12333 is concise and direct: The National Security Agency shall collect (including through clandestine means), process, analyze, produce, and disseminate signals information and data transmitted or received by foreign entities wholly outside the United States. It can also collect the communication between a foreign entity and a person in the US as long as it is the foreign entity that is targeted and not the US person. Very specific rules to protect the identity and privacy of the US person must be followed. I will discuss that in more detail later.

(Slide 12)

Relative to today's discussion – the media's alleged targeting of US persons by NSA - Executive Order 12333 further provides that

no foreign intelligence collection may be undertaken for the purpose of acquiring information concerning the domestic activities of United States persons unless they are agents of a foreign power, saboteurs or terrorists. A court warrant is required for any electronic surveillance of a US person. (Slide 13)

It is especially challenging to perform this mission today while simultaneously protecting the privacy, civil liberties, and rights of US persons in our internationally interconnected world since our adversaries make use of many of the same communications systems and services as our citizens and allies.

C. The Foreign Intelligence Surveillance Act of 1978 (FISA), the Patriot Act and the *Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008*

While Executive Order 12333 governs the interception of foreign communications that occur outside the US, the Foreign Intelligence Surveillance Act governs foreign communications that are intercepted on US domestic communications systems.

The Foreign Intelligence Surveillance Act was passed in 1978 following the investigations of the Church and Pike committees into the domestic intelligence activities of the CIA, FBI, US Army, NSA, IRS, and the White House during the 1950-1975 period. The

Watergate break-in and all that followed initially set off these investigations.

With respect to NSA the investigations revealed that during the period 1966-73 NSA intercepted the communications of 1,680 US citizens and groups placed on a watch list by the Intelligence Community and the Bureau of Narcotics and Dangerous Drugs.

(Slide 14)

The Foreign Intelligence Surveillance Act was meant to prevent such transgressions from being repeated and sought to strike a balance between national security needs and civil liberties.

The Senate Judiciary Committee stated the law was *"designed . . . to curb the practice by which the Executive Branch may conduct warrantless electronic surveillance on its own unilateral determination that national security justifies it,"* while permitting the legitimate use of electronic surveillance to obtain foreign intelligence information.

FISA provided a statutory framework for the use of electronic surveillance conducted in the United States for foreign intelligence purposes and established a special court, the Foreign Intelligence Surveillance Court, to ensure that activity carried out in the US be based on probable cause that the target of surveillance is either a foreign power, the agent of a foreign power, or a terrorist or saboteur.

The Court originally consisted of 7 judges but was expanded by the Patriot Act to 11 judges. All judges are chosen by the Chief Justice of the US Supreme Court.

FISA, as originally constructed in 1978, proved useful in obtaining significant foreign intelligence while at the same time protecting the 4th Amendment rights of US persons. But it did not provide all the tools that might have been useful in detecting and preventing 9/11.

The 9/11 planners and financiers overseas and their trainees and operatives in the US were successful in using US communications networks to carryout their plot undetected. The 9/11 Commission severely admonished the Intelligence Community for failing to "connect the dots".

While NSA was able to intercept a pre-attack call made by 9/11 hijacker Khalid al Midhar to an al-Qaeda safe house in Yemen, it had no way of determining his telephone number or where he was located. At that time, NSA had neither the tools, the database, nor the authority to search telephone company business records to determine the calling number and thus could not connect the dots. It turns out that Midhar resided in San Diego, California for the first six months of 2000 and undoubtedly made or received a number of calls that may well have led to other hijackers.

To correct this deficiency and other intelligence and law

enforcement shortfalls, the Congress passed two new laws:

(1*) Uniting and Strengthening America By Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (The Patriot Act)* which amended the section of the FISA dealing with "Access to Certain Business Records for Foreign Intelligence and International Terrorism Investigations" (50 U.S.C. sec. 1861) and

(2) *Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008 (2008 FISA Amendments Act).*

Each of these new acts authorized new intelligence tools that have been the focus of the current controversy centering on the National Security Agency. Let's look at them in some detail and then look at how the media has chosen to represent them.

(Slide 15)

1. Section 215 of The Patriot Act amended FISA to permit the government to obtain from the Foreign Intelligence Surveillance Court an order directing US communications carriers to provide the government with "Business Records" containing the date and time of telephone calls, the calling numbers, the numbers called, and the duration of the call, the International Mobile Station Equipment Identity Number (IMEI), the trunk identifier,

telephone calling card numbers, and time and duration of the call. This applies to calls made between the US and a foreign country and calls made entirely within the US.

NSA is not allowed to obtain the content of the call, the identity of any party to the call, or any cell-site locational information.

To search the metadata database NSA must provide a "reasonable articulable suspicion" that the "seed" phone number to be used in its search of the business records is associated with a particular foreign terrorist or terrorist organization previously identified to and approved by the FISA Court. Any other use is specifically prohibited.

Although the Business Records metadata program obviously collects an enormous amount of information, the vast majority of it is never reviewed by any person because it is not responsive to the queries limited to terrorism that are authorized by the Court.

The Court first authorized this program in 2006 and it has renewed it 34 times by 14 different Judges. All judges have found the program lawful and constitutional.

Once the business records metadata arrives at NSA, no analyst can query it until the following takes place:

(Slide 16)

An analyst must provide in writing that the "seed" telephone number to be used to query the database is based on a "reasonable articulable suspicion" and is associated with a particular foreign terrorist organization identified to and approved by the FISC for search purposes.

That proposed justification must then be approved by one of 22 designated and trained individuals at NSA. Only upon their approval can the metadata archive be queried. Technical controls preclude NSA analysts from seeing any metadata unless it is the result of a query using an approved identifier.

When the metadata is then queried it will show all numbers that may have been in contact with the identified terrorist's telephone number. Any number so identified may undergo further "contact chaining" to identify any numbers in contact with it. That process may be repeated one more time for any numbers found in contact with the second set identified.

By analyzing the metadata in that way NSA can determine whether known or suspected terrorist operatives have been in contact with other persons who may be engaged in terrorist activities, including persons and activities within the United States.

It is an ideal tool not only for identifying those in contact with terrorists but also for locating "sleeper cells" planned to become operative at a future date.

This process also allows for the development of a historical repository of data to find or identify known and unknown operatives, some of whom may be in the United States or in communication with US persons. This historical data may be kept for 5 years.

The results of these queries are stored in another database and available only to analysts trained in the restrictions on handling and dissemination of metadata results. The analyzed results are reported to the FBI and the CIA.

Between 2006 and late 2008, 277 reports tipping a total of 2,883 telephone numbers were so provided. In 2012, slightly fewer than 300 telephone numbers met the "reasonable articulable suspicion" criteria and they resulted in a far larger set of telephone numbers tipped to the FBI and CIA

The FBI investigates the domestic numbers tipped to it by NSA and identifies the subscribers of those numbers. If, through further investigation the FBI develops probable cause to believe an agent of a foreign terrorist element is using a number in the US, the FBI can then apply to the Foreign Intelligence Surveillance Court for a warrant to authorize the interception of

the contents of communications to and from that number. *NSA does not intercept any domestic phone numbers in this program.*

(Slide 17)

The business records metadata program is subject to an extensive regime of oversight and internal checks monitored internally in NSA by the Inspector General, the General Council, The Director of Compliance, and and externally by the Department of Justice, the Foreign Intelligence Surveillance Court, the Congress, and the Director of National Intelligence.

In spite of this rigid compliance program, mistakes did occur.

Most of the mistakes were identified in December 2008 and were the result of human error or highly sophisticated technology issues. In the initial days of the program there were 8 major software systems or process components and 248 subcomponents involving the business records metadata workflow

Needless to say, there was a lack of shared understanding among key mission, technology, legal and oversight elements of the full complexity of the program to include its implementation and end-to-end design. *Not a single one of the mistakes came from any intentional circumvention of the Courts direction and none of them resulted in spying on US persons.*

Following a full investigation of these issues and to strengthen internal monitoring and control, it was then that the NSA established the position of Director of Compliance supported by a staff of 300 people to monitor the process 24 hours a day, seven days a week.

All problems were fixed by June 2009 and the program has been reauthorized by the Foreign Intelligence Surveillance Course ever since. The last authorization took place on 11 October 2013.

(Slide 18)

2. The second new tool given to the NSA came from Section 702 of the FISA Amendment Act of 2008. Sector 702 allows the collection, including content, of exclusively foreign targets whose communications flow through American communications hubs.

Why do foreign communications flow through US hubs? Simply stated, modern communications routing technology continuously searches for the quickest path to route the worlds ever increasing volume of communications traffic at every nanosecond of time.

This results in surprising and unpredictable paths so that, for example, a message passed from an al-Qaeda element in Yemen to Alman al-Zawahiri in Pakistan might actually be routed through

the US. This happens far more often than you might think.

(Slide 19)

In allowing for NSA to target these foreign communications routed through the US, *Section 702 prohibits NSA from targeting any person known at the time of the collection to be located in the US and no US person, inside or outside the US, may be targeted.*

The Attorney General of the US and the Director of National Intelligence must authorize collection of these communications jointly after obtaining approval from the Foreign Intelligence Surveillance Court. The Attorney General and DNI authorization is valid for one year, after which it must be renewed with the Court.

NSA cannot target anyone under the Court-approved procedures unless there is an appropriate and documented foreign intelligence purpose for the collection, e.g., counterterrorism, counterintelligence, WMD, activities of foreign powers, etc. *Neither can foreign persons overseas be targeted without a valid foreign intelligence purpose.*

Under Section 702, NSA collection of foreign communications comes from two different sources.

One, providing voice, text, video, and digital network information

comes from eight major internet service providers responding to a court order to provide that data to NSA.

The second source, which NSA refers to as "upstream communications" provides raw data acquired prior to being processed by any Internet provider. It is this "upstream" source that has caused NSA problems with the Court.

(Slide 20)

What the "upstream" data involves are packet communications containing "multiple communications types" of many different subscribers in a single stream of data. When NSA targets a single foreign party in that stream, say a known terrorist, and the stream is downloaded, it contains all other communications present in it as well.

It is the perfect example of inadvertent or unintended collection, some of which inevitably contains the communications of US persons, the presence of which could not be determined in advance. Although these US communications can be later separated, segregated and minimized, they cannot be eliminated prior to downloading. This of course presents NSA with 4th Amendment issues as it has inadvertently collected the communications of US persons that the Court has prohibited it from acquiring.

Let me describe how packet switching works (slides 21 & 22).

In May 2011, when it first grasped the legal significance of what was happening, NSA bought this issue to the attention of the Court. The Court gave NSA credit for disclosing the problem but nevertheless severely chastised the agency for misleading the Court in its previous descriptions of the program and thus violating the Court's order.

The Court found that NSA's minimization procedures for the "upstream" collection were not, in some respects, consistent with the FISA statue. Several months of dialogue between NSA and the Court followed until a resolution was reached and the problem resolved. NSA also made a corporate decision to destroy all the "upstream" data previously collected.

A complicated set of minimization procedures for the "upstream" data protecting US persons can best be simplified as:

> **Wherever they are found, all domestic communications will promptly be destroyed unless the Director of NSA specifically determines, in writing, that the communication is legitimate foreign intelligence, contains evidence of a crime, or contains information pertaining to a threat of serious harm to life or property.**

Like the business records metadata process, collection of intelligence information under Section 702 is subject to an extensive oversight regime involving NSA, Department of Justice, Director of National Intelligence, Foreign Intelligence Surveillance Court, and the Congress. –

(Slide 23)

The Attorney General and the Director of National Intelligence must provide exhaustive semi-annual reports assessing compliance with targeting and minimization procedures. These reports, along with Court opinions and an additional semi-annual report by the Attorney General are provided to the Congress.

The detailed information provided by these reports provides an unprecedented degree of accountability and transparency. A separate Senate Select Committee on Intelligence investigation conducted between 2008 and 2012 found:

> **"Through four years of oversight, the Committee has not identified a single case in which a government official engaged in willful effort to circumvent or violate the law."**

IV. Intelligence Value of the NSA Programs - (Slide 24)

As much as they might like to, intelligence agencies do not

normally talk about their successes as doing so only alerts their targets and thus makes it more difficult to repeat the successes.

That is most certainly true for NSA but the current situation has forced them to tell us, at least in general terms, how the information they have been able to provide has thwarted a number of terrorist plans.

For example:

While monitoring the activities of al-Qaeda terrorists, NSA intercepted an email about a recipe for explosives from a terrorist located in Pakistan communicating with an individual who the NSA believed to be located in the US.

NSA immediately tipped the FBI and the FBI subsequently identified the individual as Colorado-based Najibullah Zazi and provided NSA with Zazi's telephone number for use with the business records metadata program.

Obeying the required Court procedures, NSA ran his number against the metadata database, passing lead data back to the FBI. That led to the identification of a co-conspirator. The FBI tracked Zazi as he travelled to New York to meet with his co-conspirators where they were planning to bomb the New York City subway system. Zazi and his co-conspirators were arrested and the plot thwarted.

Communications collected under Section 702 have provided insight to terrorist networks and plans, including specific terrorist organizations strategic planning efforts. They have also contributed to successful operations to obstruct proliferation of weapons of mass destruction technologies, cyber threats and specific potential computer network attacks.

NSA considers it its most significant tool for the detection, identification and disruption of terrorist threats to the US and around the world. Its importance is finally highlighted by the fact that the intelligence it provides consistently constitutes the greatest contributor to the President's daily intelligence briefing.

The business records metadata program and the Section 702 program have provided information successfully disrupting 54 terrorist events in the US and abroad. Thirteen of these were in the US, 25 in Europe, 11 in Asia, and 5 in Africa.

V. Media Reporting on NSA

The frequent and almost totally negative and unbalanced media reports on the operational activities and capabilities of the NSA, based on the voluminous data stolen by Edward Snowden from NSA's files, are what led me to offer this lecture. Too many of these reports, either in their headlines or

in the body of the reports are worded in a manner that creates deep suspicion that NSA is deliberately spying on Americans.

Let's review some of those reports.

1. **<u>From the New York Times</u>**

   a. June 20, 2013 - ***Documents Detail Restrictions on N.S.A. Surveillance***

   Now that is a harmless and accurate title, but let's look at its first two paragraphs:

> ***. . . President Obama, top intelligence officials and members of Congress have repeatedly assured Americans that they are not the targets of N.S.A.'s sweeping electronic collection system.***
>
> ***But as experts on American intelligence knew, that was not the whole story. It left out what N.S.A. officials have long called 'incidental' collection of Americans' calls and e-mails – the <u>routine capture of Americans' communications</u> in the process of targeting foreign communications.***

   If that does not yet leave you looking over your shoulder, just wait.

b. August 8, 2013 - *N.S.A. Said to Search Content of Messages to and From U.S.*

That is certainly true for the Section 702 program intercepting foreign communications passing through the US as I have described earlier. But here is the lead sentence:

The National Security Agency is searching the contents of vast amounts of American's e-mail and text communications into and out of the country, hunting for people who mention information about foreigners under surveillance, according to intelligence officials.

That statement was blatantly false and I was baffled as to how the Times could come to that conclusion. It turns out the Times report was based on a Guardian report that actually made no such statement. The Guardian report was its summarization of two legal documents leaked by Snowden that described the Attorney General's procedures related to the Section 702 program I discussed earlier. Two major objectives of these procedures were to ensure the 702 program acquired only foreign communications and that any incidentally acquired communications of US persons were segregated, protected, and minimized.

c. September 28, 2013 – *N.S.A. Gathers Data on Social Connections of U.S. Citizens*

Now this one is really scary. How in hell did the NYT come to that conclusion? Here are some of the statements in the article.

Since 2010, the National Security Agency has been exploiting its huge collections of data to create sophisticated graphs of some Americans' social connections that can identify their associates, their locations at certain times, their travelling companions and other personal information, according to newly disclosed documents and interviews with officials.

The agency can augment the communications data with material from public commercial and other sources, including bank codes, insurance information, Facebook profiles, passenger manifests, voter registration rolls and GPS locational information, as well as property records and unspecified tax data, according to the documents.

The remainder of the article had several other such statements, all showing either a complete misunderstanding and/or willful exaggeration of yet another Snowden provided document. So, what was it really all about?

The NSA document stolen by Snowden was an internal NSA

memo about new contact chaining procedures allowed for analysis of metadata on non-FISA collection acquired by NSA worldwide collection authorized by Executive Order 12333. It authorized the inclusion of data relating to US persons NSA had identified as communicating with valid foreign intelligence targets associated with terrorism, drug trafficking, counterintelligence activities, etc. In no case does it permit *diagraming social networks of U.S. citizens* who are in no way associated with foreign intelligence targets. I expect that describes 99.999999% of Americans.

2. **<u>From The Washington Post</u>**

   a. **August 15, 2013 – *NSA Broke Privacy Rules Thousands of Times per Year, Audit Finds.***
   This report is based on an internal NSA audit prepared by the Director of Compliance, a position established in 2009 and staffed by some 300 people, as I described earlier. The report is highly detailed and dedicated to identifying problems and solving them.

   The Washington Post report was equally dedicated to finding and highlighting every problem identified in the report and creating the picture of an agency run amok. When you dig deep down into the reporter's item you discover the following:

The NSA audit obtained by the Post **[from Snowden]** ***dated May 2012 counted 2,776 incidents in the preceding 12 months of unauthorized collection, storage, access to or distribution of legally protected communications. Most were unintended.***

What the Post did not describe, although other newspapers did, was that 1,904 of these incidents involved foreign cell phone users who, unknown to NSA, had entered the US and would then have to be covered under a FISA warrant. Most of the other errors were unintentional human or technical errors. ***None were intentional violations of procedures, restrictions, or law.***

The overall tenor of this Washington Post article and others by the same reporter, could only lead the reader to conclude that the NSA was totally out of control. I decided to write an email to the author to find out what he really thought about the agency.

I asked the following questions:

> ***Do you have evidence that NSA is deliberately targeting Americans with the intent to listen to all their communications?***
>
> ***Your latest report shows that they have a rather***

extensive internal monitoring effort on going. Do you believe this is just a cover-up? Or do you believe it is real, however faulted?

The tenor of your reports indicates to me that you possibly believe that the NSA is intentionally breaking the law and misleading its overseers. Is that an accurate perception?

How am I to judge all this about NSA? Should the agency be disestablished?

Surprisingly, I got an answer:

I wrote the piece as carefully as I could, with attention to the evidence. The story is complicated. The one thing that's clear is that the safeguards and oversight are not all they are cut out to be.
(Review accountability & oversight regime again –Slide 25)

b. August 21, 2013 – ***NSA Gathered Thousands of Americans' E-mails Before the Court Ordered it to Revise its Tactics.***

This entire report relates to the problem NSA had with its "upstream" collection containing "multiple communication types" contained in packet communications that I described earlier. The

author of the article went to great length to describe in full detail the FISA Court judge's justifiable and hard criticisms of NSA for not informing the Court earlier of the problem and, in fact, giving him incorrect descriptions in their earlier reports.

The Washington Post report also provided access to the Court's 85-page report (a Snowden item). Well, I read the entire report. Here is also what the judge said that never found its way into the Post's report.

(Slide 26)

"Therefore the Court has no reason to believe that NSA, by acquiring Internet transactions containing multiple communications, is targeting anyone other than the user of the tasked selector". **(The tasked selector is the foreign target.)**

(Slide 27)

"Given that NSA's upstream collection devices lack the capacity to detect wholly domestic communications at the time an Internet transaction is acquired, the Court is inexorably led to the conclusion that the targeting procedures are 'reasonable designed' to prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States."

I sent an email to the Post's reporter asking why these statements were not included in the report. I never got an answer.

There are many, many more misleading media items such as these, but I think you get the point.
(Slide 28)

Let me now summarize what I have tried to illustrate to you about my former employer, the real National Security Agency – not the one the media would like you swallow.

(Slide 29)

First, numerous media reports to the contrary, the National Security Agency is a foreign intelligence organization and does not spy on you or any other US person. It has no authority to do so, it has no responsibility to do so and it is illegal for it to do so. And NSA spends great effort to ensure it stays within the law. If it makes a mistake, it voluntarily reports it.

(Slide 30 – Accountability & Oversight again)

Second, there is an extensive oversight regime monitoring NSA in the executive, legislative, and judicial branches of our government. All agree that they have not found a single case of NSA consciously and deliberately monitoring, targeting, or

intercepting the calls of US persons.

I hope you take this message home with you today and that it helps you better evaluate what you read in the newspaper, see on TV, read on the Internet, and hear on the radio or what some others might say.