Testimony of

James A. Baker

April 23, 2008

Statement of James A. Baker
before the
Committee on the Judiciary
United States Senate

April 23, 2008

I. Introduction

Mr. Chairman and Members of the Committee: Thank you for the opportunity to appear here today to discuss National Security Letters (NSLs) and other legal authorities that the government uses to obtain what I will refer to as "non-content information" or "metadata." I define those terms below. In my testimony today, I will endeavor to place the debate about NSLs in the context of the larger legal regime pursuant to which the government collects metadata from a wide variety of sources, and discuss how the government actually uses various legal tools to obtain metadata. In order to understand what changes need to be made to the NSL statutes, it is important to understand how they fit into the larger legal structure that authorizes the collection and use of metadata.

The issues the Committee addresses today are of the utmost importance. As discussed below, the ability of the United States Intelligence Community and law enforcement agencies to collect, retain, and use metadata in an efficient and effective manner that is consistent with American law and values is critical to protecting our liberty and our security in the 21st Century.

I believe that S. 2088, The National Security Letter Reform Act of 2007, frames many of the key issues that Congress must address regarding metadata. The bill contains several important improvements to the existing laws governing NSLs and other legal provisions regarding the collection of non-content information. Although the bill makes important changes to the NSL statutes, as discussed below, I believe that additional changes are needed. In particular, in my view Congress should scrap the existing NSL structure and create instead a "national security subpoena" that has the following features: it must be simple and efficient to use; it must be comprehensive in its scope; its use must be subject to robust oversight mechanisms; and its use must be subject to court-approved procedures that require minimization of the acquisition, retention, and dissemination of the metadata that the government obtains, including rules regarding the destruction of collected information after an appropriate time-period. After describing what I mean by non-content information and metadata, I will comment on the existing legal structure and then elaborate on what changes I think are needed.

II. Metadata

"Metadata" refers to non-content information about communications and activities rather than the actual substance, or "content," of the communications or private activities. Metadata refers to information about a broad array of human activities. It includes information about communications (such as the date, time, and duration of a telephone call), credit card and other financial information, hotel records, airline reservation and frequent flyer records, car rental records, and many other categories of data about our day-to-day activities - where we go, what we buy, and with whom we communicate - and is usually held by third parties such as telecommunications companies, banks, and other private or governmental institutions. As some have said, metadata is information about information, and includes any type of data about an activity that is not itself a substantive communication or a recording of an activity that takes place strictly in private. Metadata would not include the actual words spoken during a telephone call, the subject line or message contained in an email, or a videotape of activities that take place in the privacy of a home. Generally speaking, the Fourth Amendment to the United States Constitution protects the content of communications and other private activities but does not protect non-content information. Even though metadata is not protected by the Fourth Amendment, many people regard it as sensitive and the collection of it as intrusive, which is one of the reasons that Congress has protected certain types of metadata from disclosure through a variety of statutes, such as the Right to Financial Privacy Act (RFPA) and the Electronic Communications Privacy Act (ECPA).

To sum up, metadata generally is not protected by the Fourth Amendment. But some types of metadata are protected in various ways by federal statutes.

Although we are focusing on the NSL statutes today, there are several other legal provisions that regulate the manner in which the government may obtain and use metadata. These include the Foreign Intelligence Surveillance Act (FISA) pen register and trap and trace statute (50 U.S.C. §§ 1841-1846), the criminal pen register and trap and trace statute (18 U.S.C. §§ 3121-3127), certain provisions of the Electronic Communications Privacy Act (ECPA) (see, e.g., 18 U.S.C. § 2703(d)), and section 215 of the USA PATRIOT Act, as amended (50 U.S.C. §§ 1861-1862). Congress also should review these statutes to determine whether they represent an appropriate balance between liberty and security today. These statutes provide the government with very useful tools for obtaining metadata pursuant to court orders. In some instances, it is highly desirable from both a privacy and security perspective for the government to be required to obtain a court order before collection can begin and for the collection to take place under the supervision of the court; in others, this may represent too cumbersome a process.

At a minimum, Congress should consider amending federal law to require that the government adhere to FISA court-approved minimization procedures with respect to the acquisition, retention, and dissemination of metadata collected pursuant any authority for national security purposes, including NSLs, section 215, the pen register/trap and trace provisions, ECPA, grand jury subpoenas, and voluntary disclosures. Section 215 currently requires minimization of the retention and dissemination of collected information, but not the acquisition of such information; similarly, S.2088 only requires minimization of retention and dissemination - not acquisition - of information the government obtains from NSLs only. I address these authorities below as part of the overall scheme under which the government obtains metadata.

III. Overview of the Current Legal Structure

The current legal regime governing the collection and use of metadata is flawed in many respects and must be changed because it places both our security and our liberty at risk. In critiquing and analyzing the current structure and assessing what should be done, it is important to keep in mind the FBI special agents and other intelligence officers who must actually use these tools in fast-paced and potentially high-stakes investigations where it can be very difficult to understand the nature and scope of a threat, or even to know whether a threat actually exists. Metadata can provide investigators with valuable information about the communications, financial, and other links between individuals who make up networks of spies or terrorists; provide investigators with the means to confirm information that they obtain from human sources and informants; and learn basic information about the identity and activities of individuals who are suspected of engaging in unlawful activity. Metadata analysis can represent a less intrusive way of assessing whether individuals are implicated in terrorist or espionage activities, or for determining that they are not involved in such activities and closing investigations of them. The intelligence officials that we charge with protecting our freedom and security are entitled to have available to them metadata collection tools that allow them to do their jobs quickly and effectively without fear of violating the law or the constitutional rights of the people they are sworn to protect. Our current legal structure does not achieve that objective.

The major flaws in the current structure flow mainly from the fact that it is extremely complex, difficult to understand, and hard to implement correctly. This complexity manifests itself in several ways. First, there are often many tools that investigators can use to obtain the same thing. For example, by my count there are at least eight distinct legal tools for collecting telephone call dialing records, such as the numbers involved in a call, and the date, time, and duration of the call. The collection and analysis of such records has been a standard investigative technique for many years for intelligence and criminal investigators in all types of cases, such as investigations of drug dealers, mafia kingpins, white-collar criminals, and terrorists.

The numerous legal tools that are available to investigators differ in important ways. Some of these differences flow from the fact that Congress shaped some of the tools mainly for intelligence investigations, and some were enacted mainly for criminal investigations. In particular, for some tools investigators must demonstrate an adequate connection to an intelligence (or at least national security) investigation and for others they must show a connection to a criminal investigation. Some tools require investigators to go to the Foreign Intelligence Surveillance Court (FISC or FISA court) for authorization while others permit investigators to go to any federal district court. Some require investigators to seek the approval of a federal criminal prosecutor but not a Department of Justice attorney whose responsibilities are intelligence in nature. In reality, however, the FBI now generally treats all national security investigations as just that - national security cases that may have intelligence and/or criminal aspects rather than separate intelligence and criminal investigations.

The tools also differ in the legal standards that investigators must meet. Returning again to telephone dialing records as an example, some tools require investigators to show probable cause, some require relevance to an appropriate investigation, and some require demonstrating specific and articulable facts showing that there are reasonable grounds to believe that the

records sought are relevant and material to an ongoing criminal investigation. I discuss these legal standards in somewhat more detail below.

Another significant difference among the tools is their scope. Investigators can use some tools to obtain a wide variety of documents, books, records, or other tangible things (such as grand jury subpoenas and orders under section 215 of the USA PATRIOT Act), while others are much more limited in scope (such as NSLs, which are limited to certain types of communications and financial information). Section 215 is the only metadata tool designed specifically for national security investigators that is comprehensive in scope. Unlike a grand jury subpoena, which only requires the approval of a federal prosecutor, section 215 requires the advance approval of a FISA court judge. Congress should note that this set of circumstances creates incentives for FBI special agents to seek to use grand jury subpoenas whenever possible in order to get around the scope limitations of the NSL provisions and, at the same time, avoid the requirement and added hassle of going to a federal judge.

The tools also differ with respect to the protection they afford to the integrity of the investigation. Some tools permit the government to require the recipient not to disclose the fact that it received an order or a directive, while tools others do not. Such non-disclosure provisions raise several significant legal questions, but, at a minimum, investigators must consider whether such provisions are available when considering whether to implement a particular tool.

In addition, the tools differ with respect to nature and scope of the oversight mechanisms in place to ensure compliance with the law. As noted above, some tools require the advance approval of a federal judge and are subject to ongoing monitoring by the court; in other instances FBI officials issue authorizations on their own with no judicial oversight. The government must report on its use of some tools on a regular basis to Congress, while there is no similar reporting requirement with respect to the use of other tools that can be used to obtain the exact same metadata. For example, pursuant to Congressional mandate, the Inspector General of the Department of Justice has conducted extensive oversight of the FBI's use of NSLs and section 215 of the USA PATRIOT Act and issued lengthy reports regarding those matters. In contrast, the FBI regularly uses federal grand jury subpoenas to obtain the exact same type of information available to it through NSLs and 215 orders, and yet the Inspector General has, to my knowledge, not issued any public reports regarding the FBI's use of subpoenas in national security cases even though the implications for the privacy and civil liberties of Americans with respect to the acquisition and use of the metadata are the same.

Another critical difference among the various investigative tools is that some tools require the implementation and use of minimization procedures, or place other restrictions on use of the collected information, while others do not. For example, minimization rules are required for metadata collected pursuant to a section 215 order, but are not required for the same metadata collected pursuant to an NSL. The FBI can also use a grand jury subpoena to obtain the same metadata that it gets from an NSL or a section 215 order, but no minimization procedures are required by statute for information acquired pursuant to a grand jury subpoena, although they may be required by Attorney General guidelines. To be sure, Rule 6 of the Federal Rules of Criminal Procedure limits disclosure of information obtained pursuant to a grand jury subpoena, but such a requirement cannot be said to constitute minimization procedures.

The complexity and variability of the legal tools available to collect and use metadata makes it more likely that investigators will make mistakes that put our security and/or our liberty at risk. For example, it is difficult to effectively train intelligence investigators, agency lawyers, and even smart, energetic law students about the rules for, and risks and benefits of, using the various tools. It also makes it more difficult to conduct proper oversight of the government's acquisition and use of metadata because it can be difficult to determine exactly what authority investigators were relying on to obtain the data. Indeed, because agencies commingle data in databases that they collect from a variety of legal authorities, it is difficult for oversight officials to figure out what is going on and assess whether any violations have occurred. Moreover, as noted above, some tools are subject to extensive external oversight while others are not.

In addition to posing risks to our liberty, the complexity of the regime also poses significant risks to our security. There is a risk that investigators will hesitate to use a readily available and proper legal tool in novel circumstances, or that they will become enmeshed in extensive legal wrangling and thereby fail to act promptly to prevent an attack or prevent a spy from compromising classified information because they are afraid of making a mistake, violating the law, and getting into trouble.

Thus, the current legal regime for collecting and using metadata is complex to the point of irrationality. It is not consistent with standards of effective management or good government. The American people deserve better.

IV. A National Security Subpoena

In my view, the Intelligence Community needs a single legal mechanism for obtaining authorization to collect, retain and use metadata; it needs a national security subpoena. Investigators should be able to obtain a national security subpoena by meeting one legal standard, which in my view should be relevance to an appropriate national security investigation or to obtain certain types of foreign intelligence information as specified by statute. Only one category of approving official should issue such subpoenas; as I suggest below, that official should be a Department of Justice attorney. National security subpoenas must be comprehensive in scope; they should be available for any type of document, record, or other tangible thing that can be obtained with a federal grand jury subpoena. National security subpoenas must have appropriate non-disclosure provisions that are consistent with the needs of national security and the First Amendment.

A national security subpoena statute should have two other critical features as well - robust oversight mechanisms and a requirement for minimization procedures. Indeed, Congress should not create a national security subpoena unless it also mandates robust oversight mechanisms for the use of such subpoenas, and requires implementation of court-approved minimization procedures that direct agencies to destroy metadata after an appropriate, but limited, time period - such as five years after the date of collection. I will address oversight and minimization issues in turn.

Effective oversight of intelligence activities can be difficult. I recently wrote a piece for the Harvard Journal on Legislation that discusses some of those challenges. For purposes of my testimony today, suffice it to say that I believe that Congress should require oversight of the use

of national security subpoenas in several ways. First, intelligence investigators should be required to obtain the approval of a Department of Justice attorney - specifically, the Attorney General, the Deputy Attorney General, an Assistant Attorney General, an attorney in the National Security Division of the Department of Justice, or an Assistant United States Attorney - before issuing the subpoena. This is similar to what is required for the issuance of a grand jury subpoena and represents an appropriate balance between the need for meaningful outside review and the need for speed and agility in issuing the large number of subpoenas that are investigators are likely to seek. Agency officials and lawyers do not represent a sufficiently independent oversight mechanism, and the large number of requests for national security subpoenas will overwhelm federal courts. According to the Inspector General of the Department of Justice, the FBI issued more than 49,000 NSLs in 2006 alone. And this number does not include the number of grand jury subpoenas that the FBI requested from federal prosecutors in national security cases.

Congress must also require oversight after the government issues a national security subpoena. The law should mandate that: the Attorney General conduct regular and thorough reviews of the use of national security subpoenas, including assessments of the use of databases and other information technology systems that intelligence agencies use to store and analyze collected information and their compliance with required minimization procedures (discussed below); intelligence agencies make available to the Attorney General all records and information that the Attorney General requires in order to conduct his reviews; Inspectors General conduct periodic audits of the collection, retention, and use of metadata by intelligence agencies; and the Attorney General and the Inspectors General make periodic reports to Congress regarding the results of their reviews.

Congress must also require minimization procedures for the acquisition, retention, and dissemination of information that intelligence agencies obtain through national security subpoenas. As with minimization procedures that Congress now requires for information that agencies collect through full content FISAs, the Attorney General should approve the minimization procedures and the FISA court should review them to ensure that they adequately protect the privacy of Americans consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information. The Attorney General and the FISA court should monitor compliance with the minimization procedures. As noted above, the minimization procedures should also mandate destruction of metadata after a reasonable period of time. Although such metadata may retain some foreign intelligence value far into the future, the ability of the metadata to generate actionable foreign intelligence information decreases rapidly and the data should be destroyed after five years from the date of collection in order to limit the privacy impact on innocent Americans.

If Congress decides not to create a national security subpoena, it should, nevertheless, require that the government implement minimization procedures with respect to the acquisition, retention, and dissemination of metadata that it obtains from whatever source for intelligence purposes. As noted below, the privacy implications of the government's collection and use of vast quantities of personal data are significant. A requirement that the government implement appropriate minimization procedures would go a long way toward enhancing the privacy of all Americans without sacrificing our security. As noted above, S.2088 only includes a requirement that the government minimize the retention and dissemination of NSL information; this should

be expanded to include minimization of acquisition so that the government is required to endeavor to limit the amount of information it collects to that which is needed for investigative purposes.

V. The Appropriate Legal Standard

One of the most important things Congress must consider is the legal standard that is appropriate for the FBI or other intelligence agencies to obtain an authorization to collect metadata. As noted above, federal law currently utilizes several standards for obtaining authorization to acquire such information depending upon the legal tool that an investigative agency is deploying. These standards include probable cause, "specific and articulable facts giving reason to believe," and relevance to either a national security or criminal investigation. Prior to the USA PATRIOT Act, the essential standard for an NSL was that the FBI had to have specific and articulable facts giving reason to believe that a particular set of facts existed. My understanding is that this standard has its origins in the criminal law with regard to situations that involve a brief seizure and a relatively non-intrusive search; as noted above, the collection of metadata does not involve a Fourth Amendment search or seizure. The USA PATRIOT Act changed this standard to relevance to an authorized national security investigation. A similar change was made to the FISA business records provision by section 215 of the USA PATRIOT Act and to the FISA pen register and trap and trace statute. Relevance is, and has been, the standard applicable for obtaining criminal pen register and trap and trace authorizations and federal grand jury subpoenas.

While it is understandable that the Committee would want to consider whether to return to the pre-USA PATRIOT Act standard of specific and articulable facts for NSLs following the revelations of abuses of NSL authorities set forth in the 2007 and 2008 Inspector General reports on the FBI's use of NSLs, I urge the Committee to tread carefully in this area. The Committee could inadvertently render the NSL statutes much less useful as investigative tools and thereby hinder FBI and Intelligence Community investigative efforts to thwart the next attack, or force the FBI to seek federal grand jury subpoenas in whenever possible in national security investigations. As noted above, there is much less oversight of the FBI's use of grand jury subpoenas for national security purposes than there is for other national security investigative tools.

As previously mentioned, I recommend that the appropriate standard for obtaining an NSL or a national security subpoena is relevance to a properly authorized national security investigation or to the collection of specified foreign intelligence information. "Relevance" means having "relation to the matter at hand;" similarly the term "relevant" means "closely connected or appropriate to the matter in hand." By comparison, the Rule 401 of the Federal Rules of Evidence defines "relevant evidence" as, "evidence having any tendency to make the existence of any fact that is of consequence to the determination of the action more probable or less probable than it would be without the evidence."

The standard obviously is broad and the government can use it to justify the collection of a wide range of information. As a result, some are fearful that it will enable the government to conduct wide-ranging "community of interest" investigations or "fishing expeditions" that will result in the collection of vast quantities of information regarding innocent people who are one, two, or

three steps removed from the person who is the subject of the investigation. But national security investigations are always about trying to understand the nature of the connections between an individual who officials suspect of posing a threat to the country and others who may be involved in the suspect's threatening activities. The government needs to know whether the connections between a legitimate investigative subject and another person are innocent or nefarious. Metadata collection represents a relatively non-intrusive way of analyzing such connections.

In assessing whether relevance or some other standard is appropriate for obtaining authorization for metadata collection, it is important to recall how investigations often work. Contrary to traditional counterintelligence investigations or ordinary criminal investigations where you often start with a subject, a victim, or a crime scene, modern national security investigations instead can begin merely with a single piece of information that may or may not signify something of concern.

Take the following example: Assume that the Intelligence Community tells the FBI that a sheet of paper that has a reference to a U.S.-based telephone number was found in a raid at a location overseas where a terrorist operative was living with family members. The only thing written on the paper was the telephone number. There is no indication that the terrorist was actually in contact with that number. The FBI obviously is going to investigate that number as it is relevant to the investigation of the suspected terrorist, even though it may or may not directly "pertain" to him.

The FBI will want to obtain subscriber information about the number, but it will also want to obtain the telephone toll records to see what other numbers the target number has contacted. At this juncture, the FBI may not be able to say that the telephone numbers in contact with the target number pertain to a suspected agent of a foreign power or someone in contact with such an agent. The toll records are, nevertheless, relevant to the investigation because the FBI is trying to see whether the target number has been in contact with any numbers that the FBI or the Intelligence Community has already determined have a terrorist connection. The FBI will also begin to analyze all of the telephone numbers that the target number has contacted that were previously unknown to the FBI. Some of those numbers may be of tremendous investigative interest, such as calls to a nuclear power plant, a U.S. military base, or another sensitive facility. If that is the case, the FBI will then want to look at telephone toll records for the telephone numbers at the sensitive facilities. Again, those numbers are clearly relevant to the investigation, but the FBI may not know whether they pertain to an agent of a foreign power. As you can see, the FBI will now be looking at numbers that are three steps removed from the target number, but that are relevant to an authorized national security investigation. It could go on from there, depending upon what the toll records reveal.

Counterterrorism and counterintelligence investigations are difficult to conduct because the costs of failure are potentially very high, there is always intense pressure to act quickly, and the subjects of the investigation are commingled with the general population and often employ sophisticated tradecraft to conceal their activities and the links between them. Investigators often do not know the identity or location of the subjects or their confederates, and sometimes do not know for sure whether such operatives even exist. Metadata collection and analysis represents an effort to uncover those suspects and the links between them based upon information and

knowledge gleaned from other types of investigative activities and analysis. The only workable standard for obtaining metadata in such an environment is relevance to an appropriate national security investigation.

It is proper to question where the civil liberties protections are in all of this. There are several potential responses to this question. As discussed above, the first way to address concerns about the relevance standard is through robust oversight and a requirement for minimization procedures and data destruction. This is simple to state and easy to include in legislation, but it is difficult, time-consuming, and expensive to do in practice. It is, however, what Congress must do if it wants to ensure that there are adequate protections for the privacy of Americans in a world where the government can and does collect significant quantities of metadata about the activities of innocent Americans. Such procedures would regulate what is acquired and why, who can access the data and for what purpose, who can receive information extracted from the data and what they can do with it, and in what manner and for how long the data can be kept in government files. An appropriate oversight structure requires modern information technology systems to maintain collected data in a secure manner and monitor how it is used.

We also need adequate numbers of competent and independent oversight and compliance officials to make sure that collection authorities are not abused. We need officials whom we can trust to look over the shoulders of the collectors and analysts to ensure that they follow the rules and respect our constitutional rights. Oversight is often an afterthought and viewed as drudgery until there is a revelation of widespread abuse. We need smart people whose integrity is unquestionable consistently watching what is going on.

In addition, Congress could require an NSL or national security subpoena to be relevant to an authorized investigation to obtain certain specified types of foreign intelligence information. David S. Kris suggested this approach in testimony on April 15, 2007, before the Subcommittee on the Constitution, Civil Rights and Civil Liberties of the House Committee on the Judiciary. Mr. Kris's testimony represents a thoughtful approach to many of the issues I have discussed and I commend it to the Committee for its consideration. Mr. Kris's approach would also address a related and difficult question regarding the use of an NSL or a national security subpoena to collect "positive" foreign intelligence, such as information that is relevant to the diplomatic or economic affairs of the United States. I recommend it to the Committee on that point as well.

VI. The Need for Analytical Resources

Notwithstanding what I have said about the importance of metadata to national security investigations, it is important to note that providing effective legal tools for the collection of metadata in a lawful manner is not a panacea. Put differently, just because Big Brother sees more does not necessarily mean that Big Brother knows more. The more information the government collects, the harder it is to sort through this information to find the bad guys. This overlooked fact suggests another area of reform that should be getting at least as much attention from Congress as the scope of the collection authority.

We must ensure that we have enough of the right people in our intelligence agencies to translate, analyze, and act upon all of the intelligence information that we collect. A successful intelligence system has four essential elements: requirements, collection, analysis, and production. We have

to seek and collect the right information at the right time - that is, we want timely and accurate intelligence about the right topics - but we also need to process, store, translate, review analyze, produce, and disseminate that intelligence so that military commanders, CIA case officers, and FBI special agents can take prompt action based on it. Poor intelligence is distracting junk, and old intelligence is history.

Advanced information technology systems assist in acquiring, processing, and assessing collected information, but they cannot do the analysis on their own. Only adequate numbers of highly trained and dedicated linguists, analysts, and agents who know their targets well can draw reasonable inferences from the facts, make prudent judgments based on the quality of the intelligence available, and make sound predictions and recommendations to policy-makers.

Moreover, the task is especially hard because, as some have noted, the needle you are looking for is broken into many pieces and most of the pieces are disguised to look like hay. Spies and terrorists don't always identify themselves clearly when they are communicating, they use code words and obscure references to convey meaning, and they rely on a variety of communication modes to transmit messages. More collection will mean more dots available to connect. But intelligence officials will need to do the hard work of connecting them.

VII. Conclusion

Effective and appropriate collection and analysis of metadata is critical to our national security and the protection of our constitutional rights. As I wrote recently in the above-referenced oversight article,

As the 21st Century progresses, effective oversight of the intelligence community will become even more essential as the risks to our security and our liberty grow. It is likely that the threats we face from hostile foreign powers will only increase over time, as will the government's ability to collect vast amounts of personal information (including our private communications and information about a wide variety of our activities), store that information, and use it in furtherance of its national security objectives. Indeed, at some point in the future any human endeavor that can be represented by digital information will be recorded and stored by someone--either for commercial or public safety reasons--and sooner or later the government will want to acquire some or all of it for foreign intelligence purposes. Telephone toll records, credit card records, and other financial records already provide investigators with powerful tools to track the movements and understand the activities of individuals who are suspected of engaging in improper activities. As more human activity takes place on the Internet, and as technologies improve to enable novel forms of monitoring--for example, the use of face recognition software to track the movement of individuals in public spaces--the volume of data available to intelligence agencies will grow substantially. We will be forced to continually ask: how do we want the government to go about protecting us? And, who will watch our guardians so that they do not become a danger to our freedoms?

The Committee's hearing today is a step forward in addressing these essential questions. In the years to come, we must decide what we mean by terms such as "privacy," and how much we want the government to know about our activities in exchange for enhancing the government's ability to protect our safety.

I would be happy to address any questions that the Committee may have regarding this matter, and will make myself available to lend any assistance I can with respect to the technical details of draft legislation that the Committee considers now or in the future.

Thank you, Mr. Chairman.

1 I am appearing here today at the request of the Committee in my personal capacity and the views I express do not necessarily reflect those of my current or former employers. The Department of Justice reviewed this statement and does not object to its publication.

2 These eight methods include: (1) metadata collected as part of a full content FISA order under 50 U.S.C. § 1805; (2) a FISA pen register/trap and trace order under 50 U.S.C. § 1842; (3) a criminal pen register/trap and trace order under 18 U.S.C. § 3123; (4) a FISA business records order (section 215 of the USA PATRIOT Act) under 50 U.S.C. § 1861; (5) a disclosure order under 18 U.S.C. § 2703(d); (6) a National Security Letter (NSL) under 18 U.S.C. § 2709; (7) a federal grand jury subpoena; or (8) voluntary disclosure by an electronic communications service provider under 18 U.S.C. § 2702.

3 As noted above, investigators can obtain metadata as part of a full content FISA authorization under 50 U.S.C. § 1805. See also 50 U.S.C. § 1801(n) ("'Contents', when used with respect to a communication, includes any information concerning the identity of the parties to such communication or the existence, substance, purport, or meaning of that communication.").

4 See, e.g., 50 U.S.C. § 1804-1805 (probable cause); 50 U.S.C. § 1861 (relevance); and 18 U.S.C. § 2703(d) (specific and articulable facts).

5 See, e.g., Office of the Inspector General, United States Department of Justice, A Review of the FBI's Use of National Security Letters: Assessment of Corrective Actions and Examination of NSL Usage in 2006 (March 2008), available at: http://www.usdoj.gov/oig/special/s0803b/final.pdf ; and Office of the Inspector General, United States Department of Justice, A Review of the FBI's Use of Section 215 Orders for Business Records in 2006 (March 2008), available at: http://www.justice.gov/oig/special/s0803a/final.pdf.

6 Of course, grand jury subpoenas do not have the same non-disclosure provisions as the NSL statutes or section 215 of the USA PATRIOT Act that raise First Amendment concerns.

7 I discuss the relevance standard in greater detail below.

8 In addition, Congress may want to consider whether to permit agencies other than the FBI to use such national security subpoenas. That is a complex and important question that will require careful evaluation and is beyond the scope of my written testimony today.

9 See James A. Baker, Symposium Introduction - Intelligence Oversight, 45 Harvard Journal on Legislation 199 (Winter 2008), available at: http://www.law.harvard.edu/students/orgs/jol/vol45_1/baker.pdf.

10 This list intentionally does not include attorneys who are assigned to the FBI or other investigative agencies for the reasons discussed below.

11 Congress could also consider requiring that national security subpoenas be issued under the authority of the FISA court in order to provide for ongoing court monitoring of the subpoena process similar to what occurs with respect to grand jury subpoenas.

12 See, e.g., Terry v. Ohio, 392 U.S. 1, 21 (1967)(". . . in justifying the particular intrusion the police officer must be able to point to specific and articulable facts which, taken together with rational inferences from those facts, reasonably warrant that intrusion.").

13 See note 2 above.

14 See, e.g., United States v. R. Enterprises, Inc., 498 U.S. 292, 301 (1991) ("[W]e conclude that where . . . a [grand jury] subpoena is challenged on relevancy grounds, the motion to quash must be denied unless the district court determines that there is no reasonable possibility that the category of materials the Government seeks will produce information relevant to the general subject of the grand jury's investigation.").

15 Should Congress decide not to create such a subpoena but merely reform the existing NSL statutes, the appropriate standard is still relevance in my view.

16 See Merriam-Webster's Online Dictionary, available at: http://www.merriam-webster.com/dictionary/relevance.

17 See Compact Oxford English Dictionary, available at: http://www.askoxford.com/concise_oed/
orexxlevant?view=uk. By comparison, Black's Law Dictionary defines "relevant" as:

Logically connected and tending to prove or disprove a matter in issue; having appreciable probative value -- that is, rationally tending to persuade people of the probability or possibility of some alleged fact." Cf. MATERIAL (2),(3) "The word 'relevant' means that any two facts to which it is applied are so related to each other that according to the common course of events one either taken by itself or in connection with other facts proves or renders probable the past, present, or future existence or non-existence of the other." James Fitzjames Stephen, A Digest of the Law of Evidence 2 (4th ed. 1881).

19 Black's Law Dictionary (8th ed. 2004).

20 See note 9 above.

21 See, e.g., "Remarks and Q&A by the Principal Deputy Director of National Intelligence Dr. Donald Kerr, 2007 GEOINT Symposium, Sponsored by the United States Geospatial Intelligence Foundation," October 23, 2007, available at: http://www.dni.gov/speeches/20071023_speech.pdf:

And that leads you directly into the concern for privacy. Too often, privacy has been equated with anonymity; and it's an idea that is deeply rooted in American culture. The Long Ranger

wore a mask but Tonto didn't seem to need one even though he did the dirty work for free. You'd think he would probably need one even more. But in our interconnected and wireless world, anonymity - or the appearance of anonymity - is quickly becoming a thing of the past.

Anonymity results from a lack of identifying features. Nowadays, when so much correlated data is collected and available - and I'm just talking about profiles on MySpace, Facebook, YouTube here - the set of identifiable features has grown beyond where most of us can comprehend. We need to move beyond the construct that equates anonymity with privacy and focus more on how we can protect essential privacy in this interconnected environment.

Protecting anonymity isn't a fight that can be won. Anyone that's typed in their name on Google understands that. Instead, privacy, I would offer, is a system of laws, rules, and customs with an infrastructure of Inspectors General, oversight committees, and privacy boards on which our intelligence community commitment is based and measured. And it is that framework that we need to grow and nourish and adjust as our cultures change.

I think people here, at least people close to my age, recognize that those two generations younger than we are have a very different idea of what is essential privacy, what they would wish to protect about their lives and affairs. And so, it's not for us to inflict one size fits all. It's a need to have it be adjustable to the needs of local societies as they evolve in our country.

Eventually, we can only hope that people's perceptions - in Hollywood and elsewhere - will catch up.