Written Questions of Senator Patrick Leahy,
Chairman, Senate Committee On The Judiciary
To David Medine, Nominee for Chair, Privacy and Civil Liberties Oversight Board

Hearing on "Nominations to the Privacy and Civil Liberties Oversight Board"

Held April 18, 2012

Data Retention

On March 22, the Director of National Intelligence and the Attorney General jointly released new guidelines governing the acquisition and retention of data by the National Counterterrorism Center (NCTC). Under these new guidelines, it is now conceivable that the NCTC could retain vast amounts of data regarding U.S. citizens for up to five years – well beyond the six months that was allowed under the previous guidelines. The new guidelines specifically state that the Privacy and Civil Liberties Oversight Board shall have "access" to all relevant NCTC records, reports, and other material relevant to its oversight of NCTC. However, the guidelines do not require any of the oversight and compliance reporting to go to the Privacy and Civil Liberties Oversight Board.

Mr. Medine, as Chair of the Privacy and Civil Liberties Oversight Board, how would you view the Board's role in reviewing this new policy and other emerging policy issues that involve the collection and retention of Americans' personal data?

If confirmed as Chair of the Privacy and Civil Liberties Oversight Board (PCLOB), oversight of information collection, use and retention policies, such as the recently released National Counterterrorism Center (NCTC) guidelines, would be a top Board priority. The accumulation of vast quantities of personal information by the government raises both privacy and civil liberties concerns. PCLOB, if reestablished, would be proactive in overseeing these types of guidelines, gathering enough information to make an informed judgment about whether the program appropriately takes into account privacy and civil liberties concerns. This would be the case whether or not the guidelines contain their own oversight or compliance reporting mechanisms.

In 2008, the Department of Homeland Security issued Fair Information Practice Principles (FIPPs). These FIPPs would provide a useful starting point for the Board in analyzing whether a program, or proposed change in a program such as the extension of record keeping for up to five years, raise concerns. The FIPPs are: transparency, individual participation, purpose specification, data minimization, use limitation, data quality and integrity, security and accountability and auditing. In the case of the guidelines, the data minimization principle states that information should only be retained for as long as is necessary to fulfill the specified purpose. PCLOB, if constituted, would examine whether the expansion of recordkeeping from six months to up to five years is necessary and justified.

An important oversight consideration is the efficacy of a program. In considering when privacy and civil liberties has properly been taken into account, PCLOB would examine the goals of a program and how well it was meeting those goals. If any program involving the collection and use of American's personal information is found to be problematic, where practical, PCLOB would work constructively with the relevant agency or agencies to convey recommended changes and assess whether alternative approaches would be possible that would address privacy and civil liberties concerns while still accomplishing the program's goals.

Senator Chuck Grassley
Questions for the Record

Responses of David Medine, Nominee, to be Chairman and Member of the Privacy and Civil Liberties Oversight Board

(1) <u>Scope of the Board's Authority and Responsibilities of its Members</u>

Following the terrorist attacks on 9/11, Congress made a number of reforms in order to protect the nation from further terrorist attacks. These reforms included tearing down the artificial "wall" between law enforcement and national security cases that the Justice Department had created; passage of the USA PATRIOT Act; reforming the intelligence community; and updating the Foreign Intelligence Surveillance Act (FISA).

All told, the various reforms, recommended by the 9/11 Commission and then implemented, have strengthened our national security and have helped to prevent another major terrorist attack on U.S. soil. However, we must remain vigilant against terrorist threats and not let down our guard. That said, some have argued that all these reforms to our intelligence, law enforcement, and national security agencies have been at the cost of civil liberties and individual rights. Recognizing this concern, the 9/11 Commission recommended that Congress create the Privacy and Civil Liberties Oversight Board to oversee the new authorities granted to these agencies.

Congress also acted by passing and signing into law the Intelligence Reform and Terrorism Prevention Act of 2004, which included provisions creating the Privacy and Civil Liberties Oversight Board in statute. In 2007, legislation updated the board's statute, reestablishing it as an independent agency in the executive branch.

As President Obama waited until December 2010 to nominate two of the five Board members and other three were not nominated by President Obama until December 2011, the role of the PCLOB has yet to be fleshed out and many details of the scope of its authority remain unclear. Thus, the philosophical perspectives of the board members of the utmost importance, and your thorough answers are appreciated.

A. What is your philosophy about privacy and civil liberties, especially when considered in the context of national security, law enforcement and cybersecurity efforts?

I share the philosophy expressed by Congress in the 9/11 Commission Act:

(1) In conducting the war on terrorism, the Government may need additional powers and may need to enhance the use of its existing powers.

(2) This shift of power and authority to the Government calls for an enhanced system of checks and balances to protect the precious liberties that are vital to our

way of life and to ensure that the Government uses its powers for the purposes for which the powers were given.

(3) The National Commission on Terrorist Attacks Upon the United States correctly concluded that "The choice between security and liberty is a false choice, as nothing is more likely to endanger America's liberties than the success of a terrorist attack at home. Our history has shown us that insecurity threatens liberty. Yet, if our liberties are curtailed, we lose the values that we are struggling to defend."

B. Describe how you would view your role as a member of this Board. Specifically, do you see the position as akin to that of a judge, an advocate, an investigator or something else? And if you see yourself as having the role of an advocate, which groups or interests will you be advocating on behalf of, if confirmed?

If confirmed, my role would be to work to preserve our civil liberties and privacy while maintaining a vigorous defense against terrorism. As provided in the 9/11 Commission Act, the Board's role is to provide independent advice and counsel on policy development and implementation and oversight of regulations, policies and procedures, information sharing practices, and other executive branch actions relating to efforts to protect the Nation from terrorism. I see myself as an advocate for preserving America's liberties and not for any special interest groups.

C. Do you believe that your work on the Board must be impartial and neutral? Or do you believe that in carrying out your work, you would be free to have empathy for certain positions or groups?

If confirmed, I believe my work on the Board must be impartial and neutral.

D. In the area of privacy and civil liberties, do you have any heroes or role models? And if you do, who are they and why are they your heroes or role models?

No.

(2) <u>Views on Duplication Existing Government Privacy and Civil Liberties Efforts</u>

The Board was created in the Intelligence Reform and Terrorism Prevention Act of 2004, as amended in 2007. The same legislation also created the Office of the Director of National Intelligence (ODNI). And consistent with the provisions of the Act, within ODNI there is an Office of Privacy and Civil Liberties. And the Department of Justice, as required by its 2005 reauthorization, has a Chief Privacy and Civil Liberties Officer with a supporting office. The Department of Homeland Security has a statutorily created Office of Civil Rights and Civil Liberties and a separate Office of Privacy. And the Department of Defense has a Privacy and Civil Liberties Office, as well as the State Department, and other departments and agencies. The Board's authorizing legislation provides that the Board will "receive reports from" other similar offices in the Executive Branch, "make recommendations" to those other offices, and "coordinate" their activities. It's not clear what the unique contribution of the Board is to this arrangement.

Although the Board has been on the books for many years, it has yet to actually function. Meanwhile, each of the relevant agencies in the war on terrorism—the Director of National Intelligence (DNI), Department of Justice (DOJ), Department of Defense (DOD), Department of Homeland Security (DHS), and others—have their own similar office. In fact, Homeland Security actually has two separate offices, one just for privacy, and one for civil rights and civil liberties - both created by the Homeland Security Act. Depending on how it is implemented, the Board is in danger of becoming another layer of bureaucracy.

I am interested in your views on what you envision your unique contribution might be, considering the vast number of privacy offices that currently exist. How do you plan to coordinate with these offices?

A. *Can you describe what the privacy and civil liberties office does at the Office of the Director of National Intelligence (ODNI)?*

   According to the ODNI website:

   The office is led by the Civil Liberties Protection Officer, a position established by the Intelligence Reform and Terrorism Prevention Act of 2004. Reporting directly to the Director of National Intelligence, the Civil Liberties Protection Officer oversees compliance with civil liberties and privacy requirements within the ODNI and ensures that civil liberties and privacy protections are incorporated into policies and procedures developed and implemented by the elements of the Intelligence Community (IC).

   Under his leadership, the Civil Liberties and Privacy Office (CLPO) ensures that the IC operates in a manner that advances national security while protecting the freedoms, civil liberties, and privacy rights guaranteed by the Constitution and federal law.

   Drawing on a broad legal and policy framework, and in concert with partner offices and institutions, the CLPO provides oversight, advice, guidance, education, and training. CLPO engages in public outreach and communication initiatives that foster awareness of how the IC accomplishes its intelligence mission while protecting Constitutional values.

   The CLPO also reviews, assesses, and, where appropriate, investigates complaints and other information indicating possible abuses of civil liberties and privacy in the administration of ODNI programs and operations.

B. *Can you describe what the privacy and civil liberties office does at the Department of Homeland Security (DHS)?*

   As DHS states on its website:

The Department of Homeland Security (DHS) divides its functions into two separate offices: the Privacy Office and the Office for Civil Rights and Civil Liberties.

The Department of Homeland Security Privacy Office is the first statutorily required privacy office in any federal agency, responsible for evaluating Department programs, systems, and initiatives for potential privacy impacts, and providing mitigation strategies to reduce the privacy impact. The mission of the Privacy Office is to preserve and enhance privacy protections for all individuals, to promote transparency of Department operations, and to serve as a leader in the federal privacy community. The office works with every DHS component and program to ensure that privacy considerations are addressed when planning or updating any program, system or initiative. It strives to ensure that technologies used at the Department sustain, and do not erode, privacy protections.

The Privacy Office:

- Evaluates Department legislative and regulatory proposals involving collection, use, and disclosure of personally identifiable information (PII);
- Centralizes FOIA and Privacy Act operations to provide policy and programmatic oversight, and support implementation across the Department;
- Operates a Department-wide Privacy Incident Response Program to ensure that incidents involving PII are properly reported, investigated and mitigated, as appropriate;
- Responds to complaints of privacy violations and provides redress, as appropriate; and
- Provides training, education and outreach to build a culture of privacy across the Department and transparency to the public.

The Office for Civil Rights and Civil Liberties supports the DHS mission to secure the nation while preserving individual liberty, fairness, and equality under the law.
CRCL integrates civil rights and civil liberties into all of the Department activities:

- Promoting respect for civil rights and civil liberties in policy creation and implementation by advising Department leadership and personnel, and state and local partners.
- Communicating with individuals and communities whose civil rights and civil liberties may be affected by Department activities, informing them about policies and avenues of redress, and promoting appropriate attention within the Department to their experiences and concerns. Investigating and resolving civil rights and civil liberties complaints filed by the public regarding Department policies or activities, or actions taken by Department personnel.
- Leading the Department's equal employment opportunity programs and promoting workforce diversity and merit system principles.

C. *Can you describe what the privacy and civil liberties office does at the Department of Justice (DOJ)?*

DOJ, on its website, describes the functions of the privacy and civil liberties office as:

The Office of Privacy and Civil Liberties (OPCL) supports the duties and responsibilities of the Department's Chief Privacy and Civil Liberties Officer (CPCLO). The principal mission of OPCL is to protect the privacy and civil liberties of the American people through review, oversight, and coordination of the Department's privacy operations. OPCL provides legal advice and guidance to Departmental components; ensures the Department's privacy compliance, including compliance with the Privacy Act of 1974, the privacy provisions of both the E-Government Act of 2002 and the Federal Information Security Management Act, as well as administration policy directives issued in furtherance of those Acts; develops and provides Departmental privacy training; assists the CPCLO in developing Departmental privacy policy; prepares privacy-related reporting to the President and Congress; and reviews the information handling practices of the Department to ensure that such practices are consistent with the protection of privacy and civil liberties.

D. *Can you describe what the privacy and civil liberties office does at the Department of Defense (DOD)?*

The DOD website provides the following description of the privacy and civil liberties office:

The mission of the Defense Privacy and Civil Liberties Office is to implement the Department of Defense's Privacy and Civil Liberties programs through advice, monitoring, official reporting, and training. The DPCLO is responsible for implementation of the Department of Defense (DoD) Privacy Program.

The Program is based on the Privacy Act of 1974, as amended (5 U.S.C. § 552a), as implemented by Office of Management and Budget (OMB) (OMB Circular A-130) and DoD regulatory authority (DoD Directive 5400.11 and DoD 5400.11-R), and is intended to provide a comprehensive framework regulating how and when the Department collects, maintains, uses, or disseminates personal information on individuals. The purpose of the Program is to balance the information requirements and needs of the Department with the privacy interests and concerns of the individual.

In discharging this assigned responsibility, the Defense Privacy and Civil Liberties Office performs multiple functions, to include:

- Developing policy, providing program oversight, and serving as the DoD focal point for Defense Privacy matters.
- Providing day-to-day policy guidance and assistance to the DoD Components in their implementation and execution of their Privacy Programs.

- Reviewing new and existing DoD policies which impact on the personal privacy of the individual.
- Reviewing, coordinating, and submitting for publication in the Federal Register Privacy Act system of records notices and Privacy Act rulemaking by the DoD Components.
- Developing and coordinating Privacy Act computer matching programs within the DoD Components and between the DoD Components and other Federal and State agencies.
- Providing administrative and operational support to the Defense Privacy Board, the Defense Data Integrity Board, and the Defense Privacy Board Legal Committee.

E. How will the Board's work differ from these offices?

The Board will bring a fresh, independent perspective to the issues addressed by the privacy and civil liberties officers, especially because four of the five board members will remain employed outside of government while serving on the Board. In the course of interacting with numerous agencies, the Board will be able to have a government-wide perspective, including a sense of how precedents established by one agency might affect other agencies. As an independent agency, the Board would not answer to the head of any of the agencies to which the privacy and civil liberties officers report. In addition, the Board's implementing statute calls upon the Board, when appropriate, to coordinate the activities of the privacy and civil liberties officers.

F. How will you ensure that you do not duplicate the efforts of these offices?

Under the implementing statute, the Board will receive and review reports and other information from the privacy and civil liberties officers. This will provide the Board the opportunity to determine what efforts and actions those officers have already undertaken to avoid duplication. In some cases, this will mean certain matters require no further attention; in others the Board will be able to build upon the work already done. Given limited budgets and the desire to not unduly burden counterterrorism efforts, it is in no one's interest to duplicate efforts.

G. If an agency, or the President himself, disagrees with input the Board provides on a particular action or policy, what will you do?

Under the Board's authorizing legislation, if a proposal is reviewed by the Board, the Board advises against implementation, and notwithstanding such advice, actions were taken to implement the proposal, the Board is required to address in reports to Congress.

H. Do you plan to make recommendations to Congress on legislation? If so, please describe how you will approach that effort.

One of the Board's key responsibilities is to review proposed legislation related to efforts to protect the Nation from terrorism. This review could involve recommending changes or additions to such legislation. As part of the Board's reporting function, there may be instances in which the Board's recommendations could include legislative proposals for Congress' consideration.

(3) <u>Preventing the Rebuilding of the "Wall" Between National Security and Law Enforcement.</u>

One of the failures of the pre-9/11 mind-set was the strict separation between law enforcement and intelligence operations. The 9/11 Commission found that the "wall" created in the 1990s in the FBI and DOJ between collection of information for foreign intelligence purposes and the use of information to prevent terrorist acts inhibited crucial information sharing. Breaking down that wall has been one of the great successes of the post-9/11 reorientation of DOJ and the FBI to terrorism-prevention, not just post-hoc crime solving. In addition, the 9/11 Commission found that the "stove-piping" of information among national security agencies was harmful to finding, tracking, and capturing terrorists. It was this "stove-piping" that prevented anyone from fully "connecting the dots" to find the 9/11 terrorists.

However, many privacy and civil liberties advocates oppose widespread sharing of information across agencies because of the fear that it allows the government to aggregate too much information about individuals. Without such capabilities, however, full pictures of terrorists will not be possible, connections among them will be missed, and terrorist networks will go undetected.

When asked about how you will ensure that none of your work contributes to the creation of a new "wall" between law enforcement and intelligence, you seemed to agree that the wall should remain down, and that you would find ways to protect both the interests of law enforcement and civil liberties. There also appeared to be agreement among the panel of nominees that you should be involved at the design stage in creating law enforcement tools that implicate privacy or civil liberties concerns.

A. *Based on your previous responses, please explain in greater detail how you plan to accomplish "finding ways to protect the interest of law enforcement and civil liberties," and "being involved at the design stage?"*

   A central function of the Board would be to strike the right balance between civil liberties and law enforcement directed toward combatting terrorism. The best way this can be done with new programs is for the Board to be involved at their design stage. For instance, if a program is proposed that might negatively impact on civil liberties, the Board might be able to work with the agency to redesign the program in a way that accomplishes the agency's goals while eliminating the civil liberties impact of the program. This could involve changes in the types of information collected or the duration for which it was retained.

B. *How will you ensure that none of your work contributes to the creation of a new "wall" between law enforcement and intelligence?*

As you note, there appears to be agreement among the nominees that a new "wall" should not be created. If confirmed, this means the Board can be expected to be sensitive to any proposals that would move in this direction and avoid contributing to the creation of such a wall.

C. *What is your view of the relationship between law enforcement and intelligence gathering?*

Both law enforcement and intelligence gathering collect information that is useful in combatting terrorism. So long as they are both collecting the information lawfully, and so long as they share the information within the approved legal framework and guidelines, such sharing should be encouraged.

D. *What is your view of the importance of information sharing between all Executive Branch agencies in order to ensure that someone can "connect the dots" to find terrorists?*

The sharing of information between Executive Branch agencies to "connect the dots" is of central importance as discussed in depth in the 9/11 Commission Report. In response, Congress, in the Intelligence Reform and Terrorism Prevention Act of 2004, created "an information sharing environment" (ISE) for sharing of terrorism information in a manner consistent with national security and with legal standards applicable to privacy and civil liberties. Demonstrating it importance, Congress has specifically required the Board to review the implementation of the information sharing guidelines required under the 2004 law.

E. *Do you oppose "stove-piping" of information by Executive Branch agencies, in order to ensure that someone can "connect the dots" to find terrorists? Please explain.*

I oppose "stove-piping" of information as it has been shown to prevent "connecting the dots." Information sharing should be done with due consideration of privacy and civil liberties concerns and consistent with legal requirements and guidelines, such as the ISE guidelines.

(4) <u>Opinions on Patriot Act & FISA Provisions</u>

The PATRIOT Act provides tools in the fight against violent acts of terrorism and was reauthorized last year. It provides authority to a court to authorize a roving wiretap to obtain foreign intelligence information not concerning a U.S. person, under Section 206. It provides authority to a court to authorize obtaining records and information under Section 215, like a grand jury subpoena. And National Security Letters can be used like administrative subpoenas, but with high-level approvals.

The FISA Amendments Act (FAA) will expire at the end of 2012. The Intelligence Committee and the Judiciary Committee will have to address reauthorization of this highly classified

national security tool soon. I am interested in your opinions about the national security and anti-terrorism tools in current law.

A. Would you vote to reauthorize the PATRIOT Act, as it now reads? If not, why not? What would you change?

B. Are there any tools authorized by the Patriot Act that you have concerns about? If so, please list those provisions and why you have concerns with them.

C. What about the Foreign Intelligence Surveillance Act (FISA) – would you vote to reauthorize it, as it now reads? If not, why not? What would you change?

D. Are there any tools authorized by the FISA Amendments Act that you have concerns about? If so, please list those provisions and why you have concerns with them.

E. Please describe when or how you have dealt with the FISA law?

In response to questions (A)- (E), Congress has devoted considerable attention to the reauthorization of the Patriot Act and prior amendments to the Foreign Intelligence Surveillance Act (FISA). These laws both provide important authority to the Executive Branch to combat terrorism. A review and comment on this type of legislation is squarely within the Board's mandate. If confirmed, I would carefully examine these laws along with the other Board members, consistent with the Board's mandate, and provide feedback to the Congress on reauthorization and potential amendment of these laws. The factors I would consider are whether the need for the government power is balanced with the need to protect privacy and civil liberties, there is adequate supervision of the use by the executive branch of the power to ensure protection of privacy and civil liberties, and there are adequate guidelines and oversight to properly confine its use. This process would address whether any of the authorized tools raise concerns. I have not had any personal dealings with the FISA law.

(5) <u>Views on the Use of the Traditional Law Enforcement Model or Military Commissions in Counterterrorism</u>

We've been fighting the war on terrorism for more than 10 years. One of the key debates in the public has been the difference between war and law enforcement. For example, the creation and operation of military commissions has been very controversial, with many people opposing their use, even for terrorists captured abroad. Some want them to be tried only in civilian courts in the United States. Other controversial topics have included detention authority, enhanced interrogation, surveillance, and drone strikes. Some people want all of these to be subject to court review and constitutional and other legal restrictions. But how one approaches these problems may be determined by whether one believes we are at war or only engaged in law enforcement. Please explain your views on the following:

A. Do you believe that we are engaged in a war on terrorism?

I believe that in appropriate cases it is permissible to use military power to combat terrorism.

B. Do you think that there are times when a law-of-war paradigm is appropriate, or should every action by the Executive Branch be governed by standard law enforcement models?

As noted in response to Question (A), I believe that there are times when a law-of-war approach is appropriate to combat terrorism.

C. If the law enforcement model is appropriate, please give some examples of why it is superior to a law-of-war model.

There may be times when the law enforcement model is appropriate. When it is, it can provide greater transparency and the perception of neutrality due to the independent decision making by a separate branch of government. This has been demonstrated in numerous successful terrorism-related prosecutions.

D. Specifically, do you think military commissions have a place in the war on terrorism? Do you think that Miranda warnings must always be given to terrorist suspects? Do you think military operations conducted abroad should be reviewed by federal courts?

There can be a place for military commissions to address certain terrorist acts. In some contexts, such as the battlefield, Miranda warnings would not be required. Likewise, in some circumstances, federal habeas corpus should be available.

(6) Views on Race and Ethnicity Relating to Terrorism Cases

On April 17, 2012, the Senate Judiciary Committee, Subcommittee on the Constitution, Civil Rights, and Human Rights, held a hearing entitled "Ending Racial Profiling in America."

A. Do you believe that focusing the limited resources of an investigative agency where they are most likely to make an impact is the best method for combating terrorism?

Yes, given limited resources, it makes sense for an investigative agency to focus on areas where it can have the most impact, if done in a legal, non-discriminatory fashion.

B. How do you address the homegrown terrorism threat, and the appropriate response to it, while completely ignoring race, religion, or ethnicity as a factor in the investigation?

One of the challenges of detecting and preventing homegrown terrorism threats is the fact that it is often not linked to any of the characteristics mentioned. As a result, the key is to develop intelligence regarding individuals and plots as the basis for taking action.

C. *While most, including me, agree that racial profiling is unacceptable, is the same true for profiling foreign nationals coming to the U.S. from certain high-risk foreign nations?*

In general, profiling of foreign nationals based solely on their point of departure to the United States is inappropriate. However, there may be intelligence regarding a plot being developed or partially implemented in a particular foreign country that could, under some circumstances, justify heightened scrutiny of visitors from that country linked to other information about the plot.

(7) <u>Targeted Killing of Anwar Al Awlaki</u>

On March 5, 2012, Attorney General Holder gave a speech on national security matters to students at Northwestern University School of Law. In his speech, Attorney General Holder discussed a number of national security issues, including the Authorization for Use of Military Force (AUMF), the Foreign Intelligence Surveillance Act (FISA), adjudication of al Qaeda terrorists via civilian courts or military commissions, and the authority to kill American citizens working for al Qaeda abroad. Specifically, in discussing the President's unilateral authority to kill an American citizen abroad, Attorney General Holder stated, "'Due Process' and 'judicial process' are not one and the same, particularly when it comes to national security. The Constitution guarantees due process, not judicial process."

Attorney General Holder further argued that "[t]he Constitution's guarantee of due process is ironclad, and it is essential – but, as a recent court decision makes clear, it does not require judicial approval before the President may use force abroad against a senior operational leader of a foreign terrorist organization with which the United States is at war – even if that individual happens to be a U.S. citizen." The Attorney General thus argued that the President has the constitutional power to authorize the targeted killing of an American citizen without judicial process.

The Board has broad jurisdiction to "review actions the executive branch takes to protect the Nation from terrorism, ensuring that the need for such actions is balanced with the need to protect privacy and civil liberties."

When asked if you believe the President has the power to target, and kill, an American citizen abroad based upon due process that does not include judicial process, you all responded that you did not have enough information about the al Awlaki scenario to make a judgment call. Regardless of the White House's failure to make its legal reasoning public, please respond to the following question based on your own opinions or beliefs.

A. *Do you believe the President has the power to target, and kill, an American citizen abroad based upon due process that does not include judicial process? Why or why not?*

Under some circumstances, I believe the President would have the power to target and kill an American citizen abroad based upon due process that does not include judicial

process. For instance, the President, as Commander in Chief, may in appropriate cases make such a decision in the event the American citizen has joined forces with foreign powers in armed conflict against the United States. There may be other situations in which this power exists and it would be within the scope of the Board's mandate to address them.

When asked if you believe the Board would have the power to declare the President's actions, in targeting American citizens abroad, a violation of constitutional civil liberties, most of you responded that you viewed your role as providing oversight and advice, and reporting to Congress. Mr. Dempsey stated that he believed the Board probably does not have the power to make "declarations." Please respond in greater detail than in your testimony to the following question, and also indicate whether or not you subscribe to Mr. Dempsey's belief that the Board does not have power to make "declarations."

B. *Do you believe the Board would have the power to declare the President's actions, in targeting American citizens abroad, a violation of constitutional civil liberties?*

The Board is authorized by statute to provide advice and counsel, including resulting findings, conclusions, and recommendations. The statute does not address the making of declarations.

C. *Do you support Attorney General Holder's public statement that due process does <u>not necessarily</u> include judicial process when it comes to national security? Which national security matters require judicial process and which ones do not?*

As noted above, there may be situations in which due process does not require judicial process in the national security context. A determination of when this is the case would be specific to particular facts and circumstances and an appropriate topic for Board review and advice.

D. *If confirmed, would you request a copy of the legal reasoning used to justify the al Awlaki killing? Would you support Congress having a copy? As this legal reasoning implicates important constitutional rights, would you support the memo being made public, with appropriate security redactions?*

If confirmed, and if the Board decided to focus its attention on the al Awlaki matter, I would favor requesting a copy of the legal reasoning to inform the Board's consideration. It does not appear to be within the Board's authority to determine whether Congress should have access to Justice Department records. As a general matter, and as reflected in the Board's authorizing statute, I would favor making information, such as the memo, public consistent with legitimate security and legal considerations.

(8) <u>Classified Information</u>

To carry out its duties, the Board is authorized to have access to information from any Department or agency within the executive branch, including classified information. To manage that classified information appropriately, the Board shall adopt "rules, procedures . . . and other

security" "after consultation with the Secretary of Defense, the Attorney General, and the Director of National Intelligence." Please elaborate on background and experience in dealing with classified information.

A. *Do you currently have a security clearance?*

No.

B. *How do you plan to hold classified information without a SCIF? Do you anticipate asking Congress to give you funds to build one?*

In order to perform its functions, the Board will require access to highly classified information that will require the use of a SCIF. If confirmed, the Board will consider options for obtaining access to a SCIF and will make appropriate budgetary requests to accomplish it.

C. *As a Board, how much time do you expect to spend reviewing classified information?*

There will be matters that the Board may undertake that would not require access to classified information or, at least, highly classified information. It is impossible to predict the amount or percentage of time that will require review of classified information until the Board has had an opportunity to convene and establish its priorities.

D. *If it's a close call in determining whether to publish sensitive national security information, on which side do you err – the side of national security or public disclosure?*

If confirmed, I would generally favor public disclosure. However I would also be sensitive to and seriously consider the potential consequences of making sensitive national security information public.

(9) <u>Scope of Constitutional Protections</u>

Currently, national security law defines a U.S person as a U.S. citizen (USC), a Lawful Permanent Resident (LPR), a U.S. corporation, or a group whose members are substantially USCs or LPRs. FISA, 50 U.S.C. 1801. Some argue that all persons found in the United States should receive the same protections under the Constitution that U.S. citizens possess.

A. *Who should be entitled to protection as a U.S. person?*

As noted, FISA contains a definition of "United States person", for FISA purposes, that includes "a citizen of the United States, an alien lawfully admitted for permanent residence (as defined in section 1101 (a)(20) of title 8), an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a

foreign power, as defined in subsection (a)(1), (2), or (3) of this section." By contrast, "United States Person" is defined in Executive Order 12333 to mean "a United States citizen, an alien known by the intelligence element concerned to be a permanent resident alien, an unincorporated association substantially composed of United States citizens or permanent resident aliens, or a corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments." If confirmed, I would consider whether and how these definitions should be reconciled in addressing the degree of Constitutional protection that should be provided to non-U.S. citizens found in the United States.

B. Do you believe that the definition of U.S. person should be broader, to include persons in the process of applying for permanent residence, or do you believe it should it be restricted to the traditional statutory definition in FISA?

I have not previously considered this issue but, if confirmed, believe it would be an appropriate topic for Board consideration.

C. If the definition of U.S. person is defined broadly, can it create problems for quickly sharing terrorism information? If not, why not?

Defining U.S. person broadly would impose burdens on the sharing of terrorism information. The Board would be in a position to address whether the benefits of a broader definition justify any such increased burdens.

(10) <u>Scope of Authority to File Amicus Briefs</u>

The Board is given very broad duties and authorities. The statute clarifies that this Board is to be treated as an agency and not an advisory committee.

A. Do you believe it is within the Board's authority and power to file an amicus brief in a case?

There is no express statutory authority for the Board to file amicus briefs. Given the Board's extensive responsibilities and limited budget, filing amicus briefs would not likely be a prudent use of the Board's resources.

B. If the answer to the above question is yes, and if it takes only three Board members to make a quorum, can the Board file an amicus brief if two members don't agree?

N/A

C. If the answer to the above question is yes, could the two disagreeing members file a brief outlining their opposing view?

N/A

D. Where in the statute do you find the authority that allows the Board to file an amicus brief?

N/A

(11) <u>Cybersecurity Legislation</u>

Many of the Cybersecurity bills include language rebuilding the wall, by limiting the use of cyber-threat information for purposes outside Cybersecurity—including national security and counter intelligence.

(1) Do you support recreating the wall as part of cybersecurity legislation?

I do not favor recreating the wall between national security and law enforcement as part of the cybersecurity legislation.

(2) Regardless of what Congress does, do you think that a wall should exist between cybersecurity information sharing to prevent cyber-attacks and law enforcement?

While I do not favor recreating the wall between national security and law enforcement, as noted in my response to Question 3 above, there would likely be a broader scope of information collected to prevent cyber-attacks that would require separate consideration, including potential use and disclosure restrictions.

(3) At the hearing, many of you stated you have not studied this issue. Mr. Dempsey stated that, if confirmed, the Board would look closely at this issue. However, Mr. Dempsey added, "Congress is going to have a say on that issue, I think, before this board comes into creation, and we will work with the authorities and decisions that Congress makes on that cybersecurity legislation." While I appreciate your willingness to study the issue and your deference to Congress, I want to know your position on certain cybersecurity related topics.

1. *Do you support private networks, service providers, and private industry sharing customer information with the Federal Government if that information evinces a cybersecurity threat or vulnerability to public or private systems? If not, why not?*

   There is clearly an important benefit to having private networks, service providers, and private industry share cybersecurity threat or vulnerability information with the Federal Government. If confirmed, I would want to consider whether there should be any limitations or protections associated with such sharing depending on the nature of the entity sharing the information, the type of information being shared and the possible use and disclosure of such information.

2. *What restrictions should be placed on information shared with the Federal Government? Should information be limited to metadata only or should it include contents of communications?*

   Depending on the nature of the information being shared, there may be greater or less need to provide associated privacy protections. For instance, there may be good reasons to accord less protection to metadata than the contents of communications.

3. *What restrictions should be placed upon cybersecurity threat information shared with the Federal Government? For example, should personally identifiable information (PII) be minimized or redacted? Should the use of this information be limited to merely address cybersecurity threats or could it be used for national security, intelligence, counterintelligence, national security, or criminal matters? If you believe it can be shared, what categories of the aforementioned purposes can it be shared?*

   Consistent with fair information practices and the utility of the information for cybersecurity protection, personally identifiable information should be minimized or redacted. Secondary use of this information could implicate a wide range of legal and policy issues calling for case-by-case review. For instance, privacy and civil liberties protections in place elsewhere should not be circumvented by collecting information for cybersecurity purposes.

4. *How long should any shared information be retained?*

   Given that the cyberthreats tend to be time-limited, the "shelf life" of such information would presumably be relatively short, making it unnecessary for it to be retained for an extended period of time.

(12) United States v. Jones

In her concurrence in the recent case, United States v. Jones, 132 S. Ct. 945, 954 (2012) (Sotomayor, J., concurring), Justice Sotomayor agreed with Justice Alito that, "at the very least, 'longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy.'"

Her concurrence then elaborated that even with short-term monitoring, "some unique attributes of GPS surveillance relevant to the Katz analysis will require particular attention." Justice Sotomayor stated that GPS monitoring "generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious and sexual associations." She further indicated that she "would take these attributes of GPS monitoring into account when considering the existence of a reasonable societal expectation of privacy in the sum of one's public movements."

A. *With respect to Justice Sotomayor's discussion of the temporal elements of the 4th Amendment, please explain your interpretation of her statements and whether or not you support her position.*

Justice Sotomayor's concurrence in United States v. Jones attempts to wrestle with the application of the Fourth Amendment to technologies that may not require a physical intrusion, going beyond the basis of the majority decision, which turned on the physical occupation of private property for the purpose of gathering information. While she and Justice Alito note, and I agree, that longer term GPS monitoring could infringe on the expectations of privacy protected under *Katz*, as duration of surveillance can change its nature, Justice Sotomayor also recognized that even short-term monitoring could implicate the *Katz* analysis. Thus, it is not clear what weight she would give to long term versus short term monitoring, as compared to the weighting of the nature of the monitoring and the type of information collected. Nonetheless, I agree with the need to carefully evaluate new technologies under the Fourth Amendment in light of temporal and other factors, as the Supreme Court has now done by extending protections in both *Jones* as well as in Kyllo v. United States, 533 U.S. 27 (2001).

B. *Do you believe the 4th Amendment has a temporal restriction? Do you believe that information that is initially acquired lawfully may become subject to 4th Amendment restrictions over time?*

Please see my response to (A). In general, information lawfully required is unlikely to become suspect under the Fourth Amendment retroactively.

(13) <u>Agency Authority</u>

The statute establishes the Board as "an independent agency within the executive branch". And the Board "shall" analyze and review actions taken by the executive branch. The Executive Office of the President is obviously part of the executive branch, and nowhere is the President excluded from the Board's review and purview.

A. *Do you believe that the Board will have the duty to review and analyze actions of the President and the Executive Office of the President?*

The authorizing statute directs the Board to review actions taken by "the executive branch" which would include the President and the Executive Office of the President.

B. *Do you believe that the Board will have the duty to review and analyze actions of the Vice President and the Office of the Vice President?*

See the response to (A).

C. *If the Board disagrees with the actions taken by the President, Vice President, or either of their offices, <u>after</u> the Board has fulfilled its duty to "advise the President… and executive branch", what options does the Board have?*

The Board has the option of reporting on the matter to Congress. In the case of proposals reviewed by the Board, the Board is required by statute to report on instances in which the Board advised against implementation and, notwithstanding such advice, actions were taken to implement the proposal.

D. *What is your understanding of the term, "independent agency within the Executive Branch"? How would you compare your authority to that of other, fully independent boards outside the Executive Branch, such as the Securities and Exchange Commission?*

Congress did not define the term "independent agency within the Executive Branch." However, given the history of the Board under prior legislation, it is clear that Congress intended the Board to engage in oversight, give its advice, provide Congressional testimony, develop and communicate its views, and issue its reports without prior review or approval by the White House. In this respect, the Board's authority is similar to boards that have been established outside the Executive Branch, such as the Securities and Exchange Commission. In contrast to some other independent agencies, the Board does not have general rulemaking or law enforcement authority.

The Board is given authorization for access to any Department, any information, any document, or any person to carry out its duties. And if that access is denied, the Board can ask the Attorney General to issue a subpoena.

E. *What recourse will the Board have if the Department of Justice is the executive branch component that is denying access to information?*

The Board's authorizing statute provides an alternative mechanism from subpoenas for addressing cooperation by the Executive Branch. When information or assistance is unreasonably refused or not provided, the Board is required to report the circumstances to the head of the relevant agency who is, in turn, required to ensure the Board is given access to the information, assistance, material, or personnel the Board determines necessary to carry out its functions.

F. *If it is the Office of the President that is denying the Board access to information, do you believe it is realistic that the Board will seek a subpoena from the Attorney General, who reports to the President?*

See the response to (E).

(14) Use of International and Foreign Law in Interpreting Privacy and Civil Liberties Issues

At the hearing, Judge Wald noted her experience with international law, citing her time as a judge on the International Criminal Tribunal for Yugoslavia. This raises the disturbing problem of judges in the United States relying on international and foreign law in interpreting the U.S. Constitution and statutes. In a number of cases, justices of the Supreme Court have cited non-U.S. laws as support for overturning U.S. laws, such as those on execution of juveniles and of the mentally handicapped. Separate and apart from the ultimate wisdom of those decisions, the fact that justices had to rely on other countries' and international organizations' opinions on legal matters, and not on the text, history, and structure of the Constitution and on American legal traditions, is concerning. In addition, as Justice Scalia has pointed out, those justices and the advocates of the use of international and foreign law only selectively cite it as relevant. They typically cherry-pick foreign and international legal decisions that support their favored policy positions, such as abolition of the death penalty, but ignore those that disagree with their positions, such as restrictions on the availability of abortion in most countries around the world.

The problem of selective use of international and foreign law in interpreting U.S. law would seem to be equally at issue for the members of the Privacy and Civil Liberties Oversight Board. Protections for privacy and civil liberties vary widely from one country to another. For example, the United States provides far more rights to the accused than most other countries. In much of Europe, defendants accused of terrorist crimes can be held for up to a week without charge or without seeing a neutral magistrate, rather than the Constitutionally required 48 hours in the United States. Likewise, virtually all European countries, as well as others around the world, require citizens to possess and carry a national identification card that must be presented to authorities upon demand. Such a requirement would be denounced in the United States, and proposals for such a card have never been successful. Laws on surveillance, leaks of classified information, and racial profiling are also far more lenient in much of the rest of the world.

At the same time, human rights advocates have greatly expanded the notion of international human rights law to cover areas of privacy and civil liberties, and they are fond of citing to international treaties, such as the International Covenant on Civil and Political Rights, as support for their attacks on U.S. law and appropriate interpretations of the U.S. Constitution. Like-minded members of international bodies, mainly law professors from around the world, such as the U.N.'s "special rapporteurs," parrot these arguments. Meanwhile, the non-democratic majority of the U.N. General Assembly passes resolutions against the United States motivated by dislike of our foreign policy and tradition of freedom and capitalism. Then human rights advocates claim that "international law" supports their positions.

A. If confirmed, do you commit that your evaluations of the legality and propriety of U.S. government actions to fight terrorism, as they relate to the protection of privacy and civil rights, will be based exclusively on the requirements of the U.S. Constitution, as interpreted by the Supreme Court, and on U.S. law, and not on foreign countries' laws or on allegations of what international law requires?

If confirmed, I would base my evaluation of the legality of counterterrorism actions based solely on U.S. law. Evaluations of the propriety of such actions would be based on U.S. standards and expectations though it could be informed by how other countries have addressed privacy concerns.

Senator Chuck Grassley
Additional Questions for the Record

David Medine, Nominee, to be Chairman and Member of the Privacy and Civil Liberties Oversight Board

(1) <u>Chairman Responsibilities:</u>

The Board's authorizing statute provides for extremely broad, vaguely-defined purposes and functions. If it were to try to do everything the statute authorizes, it would be a large bureaucracy with intrusive powers that could become a serious impediment to effective counterterrorism efforts. For example, although nominally bipartisan, it is to be run primarily by one full-time chair (a Democrat) and four part-time commissioners. It is likely that the chairman will dominate selection of the staff. The statute provides very broad authority for the board's functions.

The Board is authorized to provide advice on, and oversight of, policy development and implementation, as well as laws and regulations, of Executive Branch agencies. The board is to "continuously review" any actions by the Executive Branch. They are allowed access to <u>any</u> information they want, may compel production of documents or testimony through subpoena power, hold public hearings, report and testify to Congress, and oversee other privacy and civil liberty offices within the Administration.

A. *Please describe how you will accomplish the broad statutory mandate for the Board.*

In order for the Board to operate effectively, within its budget, and in a way that does not become an impediment to counterterrorism efforts, if confirmed, the Board members will have to carefully assess and prioritize the areas in which the Board can be most effective and add value. This will involve both oversight of targeted ongoing programs as well as providing feedback on new programs and legislative proposals. The Board will take advantage of information gathered by privacy and civil liberties officers and inspectors general so as not to duplicate their efforts.

B. Will you prioritize certain functions or subject-matter areas?

One of the first orders of business, if the Board nominees were confirmed, would be for the Board to meet and establish priorities for the types of programs it will review.

C. How large a staff do you expect to hire? What types of backgrounds will they have?

It is not possible to anticipate the size of the Board's staff until its budget is established. A critical first hire will be an Executive Director to handle the administrative aspects of starting a new independent agency. It will also be important to have staff to handle legal and ethics issues the make sure they are properly addressed. There will be professional staff to assist the Board with its oversight and advice functions. The authorizing statute provides for the Board to make use of detailees who are Federal employees. This will provide an opportunity to have the benefit of employees with extensive experience on

counterterrorism efforts and privacy and civil liberties issues from various agencies and offices. Staff hires will be made in consultation with Board members and without regard to political affiliation.

ANSWERS TO SENATOR KLOBUCHAR'S QUESTIONS FOR DAVID MEDINE

QUESTIONS FOR THE RECORD

From Senator Amy Klobuchar

"*Nominations to the Privacy and Civil Liberties Oversight Board*"

April 18, 2012

Questions for all witnesses

Question No. 1: Career Experience

You have all established very impressive careers with experience working in both public service and private legal practice.

- *Can you describe any experiences you have had in your career in balancing civil liberties with national security or other priorities?*
- *How did you go about analyzing such conflicts?*

While in private practice, I supervised two pro bono projects for the bipartisan Constitution Project that presented the opportunity to balance national security and criminal enforcement with civil liberties concerns.

In 2007, American cities had begun to install networks of video cameras in public places to address the increased terrorism threat as well as other concerns about public safety. The cameras could be equipped with technologies such as high resolution and magnification, motion detection, infrared vision, and facial recognition—all linked to a powerful network capable of automated tracking, archiving, and identifying suspect behavior. The cameras could track a person's movements throughout the city, capturing where they went, what they did, and with whom they associated, thus raising concerns about privacy, free speech and association, and equal protection. A report was prepared for the Constitution Project that balanced constitutional rights and values with legitimate law enforcement and anti-terrorism goals, by proposing guidelines for the proper management of video surveillance programs. The guidelines included requiring a clear statement of purpose for the program, conducting a civil liberties impact assessment, restricting tracking of individuals, providing public notice, and establishing safeguards to prevent abuse. This balance would permit use of video surveillance for legitimate purposes while respecting civil liberties values.

Two years later, I assisted the Constitution Project in developing a response to numerous federal agencies' use of over 100 types of labels to designate information, which did not qualify for national security classification, as sensitive but unclassified (SBU) or controlled unclassified information (CUI). There were valid reasons for some documents that did not qualify for classification to, nonetheless, be treated as sensitive with controlled access. However, the SBU or CUI systems lacked any clear standards or accountability with the counterproductive effect of limiting the ability to share such information, which could be put to use in combatting terrorism, with other agencies. The Project's report proposed that a balance be struck between openness in government and protecting sensitive information by creating common government standards and a presumption of openness, increasing access to information by other

federal agencies and the Congress, de-linking CUI identification from responding to FOIA requests, and having these requirements extend beyond terrorist-related information. This approach respected the need to protect certain sensitive information while promoting public accountability and access.

Both of these cases involved government programs with legitimate goals where the methods chosen raised civil liberties concerns. After analyzing the programs, it became clear that changes could be made and guidelines adopted that would permit the programs to proceed consistent with protecting civil liberties.

Question No. 2: Privacy Concerns in the Commercial Arena

Privacy concerns are not just present in the national security context, but also in the commercial arena and with respect to the government's regulation of commerce.

- *Can you talk about how the dynamics or considerations of privacy might be different in commercial contexts as opposed to security contexts?*
- *Specifically, how can industry, including telecommunications firms, and the government work together to improve our approach to privacy issues?*

Whenever information is collected about individuals, privacy concerns can arise, whether it is collection by the government for national security purposes or by private firms for marketing purposes. In the commercial context, there is a tension between companies' wanting as much information as possible about their customers, often to improve their ability to market new products and services, and some customers' discomfort with the collection practices employed. By contrast, in the national security context, the government seeks to collect information with the goal of detecting and thwarting potential attacks on this country and locating and bringing to justice anyone who attempts or carries out such attacks. While protecting our national security is a shared goal, there are legitimate concerns about how much information is collected by the government that could prevent or chill the exercise of civil liberties and also could be subject to abuse.

While these very disparate contexts give rise to privacy concerns, there are common approaches that can be used to address them. One effective approach is "privacy by design." The best, most efficient time to address privacy is during the design process, whether it involves a counterterrorism program or a commercial website that wants to better understand its visitors. It is possible in program design to achieve governmental or commercial goals while respecting privacy concerns. However, it is far harder to make changes to an existing program to address privacy concerns.

Another tool for protecting privacy the national security and commercial contexts is accountability. The Privacy and Civil Liberties Oversight Board is designed to serve as a check on certain governmental information collection and use practices to make sure they strike the right privacy balance by exercising its oversight authority, including gathering data on what information is being collected and how it is being used. In the commercial context, accountability can be accomplished by providing consumers the opportunity to access information collected about them. The Federal Trade Commission and other government agencies can also use their investigative and enforcement powers to conduct oversight. Self-regulatory organizations can also play an important role.

In addition to working on parallel tracks, there are opportunities for government and the industry to better protect individuals' privacy. Fair information practices (FIPs) have been developed in the private and public spheres. Industry and government could share their approaches to effectively addressing FIPs. For

instance, the Privacy and Civil Liberties Oversight Board is authorized to hold public hearings at which industry and government could collaborate on effective ways to address privacy issues.