Questions for the Record – Responses of James X. Dempsey

Question from Chairman Leahy

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. Dempsey, as a member 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?

A: If confirmed, I would recommend to the Chairman of the Board and fellow Board members that the Board view this issue within the broader context of the role and activities of the NCTC. In particular, I believe that the new guidelines on retention should be examined within the context of the full range of data that agencies share with the NCTC and how the NCTC uses that data. If confirmed, I would want to explore what other checks and balances, in addition to any specified time limit on data retention, are in place, or would be appropriate, to protect civil liberties while ensuing that the NCTC is able to fulfill its mission. On these questions, I would want to consult closely with the responsible officials at DHS, at the NCTC, and at other agencies.

Questions for the Record – Responses of James X. Dempsey

Senator Chuck Grassley Questions for the Record

(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?

A: My philosophy on this matter is the same as that expressed in the findings of Congress in Section 1061(b) of the National Security Intelligence Reform Act of 2004, as amended by Section 801(a) of 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?

A: If confirmed, I would view my role as defined in the statute establishing the Board: to provide independent advice and counsel on policy development and implementation related to efforts to protect the Nation from terrorism and oversight of regulations, policies, and procedures of the Executive Branch relating to efforts to protect the Nation from terrorism, to ensure that privacy and civil liberties are protected, as further delineated in the statute, recognizing that the Board would have to prioritize its activities and would want to avoid duplication of effort with existing privacy and civil liberties processes and offices.

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?

A. I believe that my work on the Board, if confirmed, 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?

A. My hero and role model in the area of privacy and civil liberties is now-retired Congressman Don Edwards, former FBI agent and long-time chairman of the House Judiciary Committee's Subcommittee on Civil and Constitutional Rights. Chairman Edwards exercised oversight of the FBI with the highest respect for the men and women who risk their lives to keep us safe, displaying in all his actions his dedication to the Constitution and his love for this country. If confirmed, I would strive to do the same.

(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: If confirmed, I will adhere to the directions in the statute creating the Board, which addresses relationships with the existing privacy offices in Section 1061(d)(3). If confirmed, I will strive to coordinate, collaborate and consult regularly with the privacy officers and all other relevant oversight bodies and mechanisms, to avoid duplication, including in setting the priorities of the Board.

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

A: My understanding of the work of all of the privacy and civil liberties officers is grounded in the statutory description of their functions, section 803 of the 9/11 Commission Act, which amended Section 1062 of the National Security Intelligence Reform Act of 2004.

The responsibilities of the privacy and civil liberties officers at the Office of the Director of National Intelligence include ensuring that the protection of privacy and civil liberties is appropriately incorporated in Intelligence Community policies and procedures, overseeing compliance by the ODNI with privacy and civil liberties laws, reviewing complaints of possible abuses of privacy and civil liberties in programs and operations administered by the ODNI, and ensuring that the use of technology sustains, and does not erode, privacy. Further statutory direction specific to this office is found in 50 U.S.C. 403-3d.

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

A: The Department of Homeland Security has an Office for Civil Rights and Civil Liberties and a Chief Privacy Officer. The DHS Privacy Office works with every Department 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. Responsibilities of the Chief Privacy Officer are further described in Section 222 of the Homeland Security Act of 2002, as amended, 6 U.S.C. 142. The responsibilities of the Office for Civil Rights and Civil Liberties are further described in Section 705 of the Homeland Security Act, 6 U.S.C. 345.

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

A: The Department of Justice has a Chief Privacy Officer and an Office of Privacy and Civil Liberties (OPCL). 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. The responsibiliites of the Chief Privacy Officer are described in section 1174 of Pub. L. 109-162.

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

A: The Department of Defense privacy and civil liberties office oversees programs and develops policy to protect privacy and civil liberties of more than 2.3 million U.S. Military service members (Active, Reserve and Guard), 700,000 Civilian employees, military installations, hospitals, and schools, as well as the private citizens and organizations with whom DOD interacts.

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

A. In contrast to these offices, the Board will be an independent entity, it will have a government-wide perspective, and it will focus on policies, programs and powers relating to efforts to protect the Nation from terrorism (and other matter specifically assigned to it by Congress), while those offices have a purview and responsibilities extending beyond counter-terrorism programs

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

A: If confirmed, I will work with the Chairman of the Board to ensure that the Board coordinates closely with these offices to avoid duplication. Among other steps that will promote coordination, the statute establishing the Board specifies that the Board will receive and review reports and other information from privacy officers and civil liberties officers. If confirmed, I expect that among our first activities will be to meet with these offices, and I further expect that we will meet or communicate with them on an ongoing basis, seeking their guidance on priorities

and the avoidance of duplication.

The war on terrorism requires a careful balance between aggressive counter-terrorism policies and the protection of privacy and civil liberties. We can't be so aggressive that U.S. citizens rights' are violated, but we also can't ignore effective policies that will deter and prevent terrorist acts. Most relevant agencies have a civil liberties or privacy office now, that have been debating this balance for years. So, in many ways, this Board is late to the debate.

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

A: If confirmed, in the situation described I would work with the Chairman and the other members of the Board to fulfill the directions of section 1061(e)(2)(D).

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

A: The statute creating the board states that the Board shall review proposed legislation related to efforts to protect the Nation from terrorism and advise the President and the departments, agencies, and elements of the Executive Branch to ensure that privacy and civil liberties are appropriately considered in the development of such legislation. The statute does not expressly require the Board to make recommendations to Congress on legislation. However, the statute does require the members of the Board to appear and testify before Congress upon request. In addition, the statute requires the Board to periodically submit, not less than semi-annually, reports to Congress that shall include information on the findings, conclusions and recommendations of the Board.

(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: If confirmed, I will seek ways to protect the interests of law enforcement (and national security) and civil liberties by listening carefully to law enforcement, intelligence and national security officials to understand the threats and challenges they face and the approaches that are available to them (or could be developed). I will discuss with them the full range of alternatives and work with them to determine what approach, if any, is most likely to achieve the counterterrorism objective while also protecting civil liberties. One of the best ways to achieve that balance is when a program is being designed, when the range of options is often widest. That is often the best time to build in the controls and other features that would make a program successful but also protective of civil liberties.

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

A: If confirmed, I expect to closely consult, along with other members of the Board, with both law enforcement and intelligence agencies that have a need for information from each other, to understand their needs and to directly ask them if any of our recommendations would contribute to a new wall.

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

A: Our lead federal law enforcement agency, the FBI, is also an intelligence agency, and the guidelines for FBI domestic operations promulgated by Attorney General Mukasey correctly recognize that in exercising its law enforcement, national security and foreign intelligence authorities, the FBI collects "information," which should not be stovepiped. As the guidelines state, "The major subject areas of information gathering activities under these Guidelines - federal crimes, threats to the national security, and foreign intelligence - are not distinct, but rather overlap extensively."

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?

A: It is critical that Executive Branch agencies share information in order to ensure that someone can "connect the dots" to find terrorists. The statute establishing the Board states that the Board shall review proposed legislation, regulations, and policies related to the development and

adoption of information sharing guidelines and to review the implementation of those guidelines.

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.

A: I oppose "stovepiping" of counter-terrorism information by Executive Branch agencies (recognizing that security concerns must be addressed). I believe that it is possible to promote information sharing within a framework that protects the security of the information as well as privacy and civil liberties.

(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?

A: The statute establishing the Board specifies that, in providing advice on proposals to retain or enhance a particular governmental power, the Board shall consider whether the department, agency, or element of the executive branch has established (i) that the need for the power is balanced with the need to protect privacy and civil liberties; (ii) that there is adequate supervision of the use by the executive branch of the power to ensure protection of privacy and civil liberties; and (iii) that there are adequate guidelines and oversight to properly confine its use. If confirmed, and if any question concerning the PATRIOT Act were to be considered by the Board, I would make my assessment based on all the facts, within the framework laid out by the statute establishing the Board.

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.

A: At this point, it is impossible for me to say whether, as a member of the Board, I would have any concerns about any of the tools authorized by the Patriot Act. I would note that the FBI's implementation of the authority to issue National Security Letters, amended by the Patriot Act, has been examined by the Inspector General in several reports, and the FBI has adopted further procedures for NSLs in response to the findings of the IG. Depending on any current or planned work by the IG or other offices, implementation of the NSL authority might or might not be an

appropriate subject for the Board to examine. If confirmed, and if the Board were to examine any of the tools authorized by the Patriot Act, I would proceed as described in response to question A.

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?

A: At this point, it is impossible for me to say whether, as a member of the Board, I would have any concerns about FISA. If confirmed, and if the Board were to examine any aspect of FISA, I would proceed as described in response to question A.

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.

A: At this point, it is impossible for me to say whether, as a member of the Board, I would have any concerns about the FAA. If confirmed, and if the Board were to examine any aspect of the FAA, I would proceed as described in response to question A.

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

A: I have dealt with FISA as an outsider. I have written about FISA, most recently for a volume entitled "A Journalist's Guide to National Security Law," being compiled as a joint project of the American Bar Association Standing Committee on Law and National Security and the Medill School of Journalism National Security Initiative. Between 2005 and 2008, I testified on several occasions before Congressional committees on proposed changes to FISA.

(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?

A: I believe that Congress has authorized the use of military force against Al Qaeda and its allies and that it is appropriate to use military force against foreign terrorists in other circumstances.

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?

A: Yes, there are times when a law-of-war paradigm is appropriate.

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

A: The law enforcement and intelligence models are appropriate in most circumstances inside the United States. For example, the grand jury is a very powerful information gathering tool that is not available to the military. Overseas, when cooperating with allies, especially when operating in democratic countries, a law enforcement or intelligence model may be appropriate. For example, authorities in the UK, when they have arrested a terrorism suspect, may prefer to share information and coordinate responses on both sides of the Atlantic with U.S. law enforcement or intelligence officials rather than with military officials.

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?

A: I have no opinion on military commissions – it is simply not a subject I have studied. In terms of the application of Miranda warnings in the context of terrorism, I also have not studied it and do not have an opinion about what must always happen. I am not familiar with any theories under which military operations conducted abroad should be reviewed by federal courts. If I am confirmed, and if any of these issues comes before the Board, I will give it full and fair consideration, carefully studying the relevant law and consulting closely with relevant entities.

(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?

A: Yes.

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?

B: I do not have a theory on how to address the homegrown terrorist threat, except to say that the response must be guided by relevant intelligence. I understand that the homegrown threat is diverse, ranging from Major Nidal Hassan to the 5 anarchists arrested recently in an alleged plot to blow up a bridge near Cleveland. As a general matter, it seems to me that, since terrorism is often carried out by those motivated by religious or other ideology, it is impossible to completely ignore ideology in responding to it.

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?

A: I agree that racial profiling is unacceptable. That being said, I would not say that it is "profiling" to consider, for purposes of screening at the border, arrival from or transit through a high-risk foreign nation.

(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?

A: This is not an issue I have studied or carefully considered before. The power referred to is an extraordinary power, but I always hesitate to offer opinions about momentous matters that I have not carefully considered. My assumption is that many factors would come into play in determining what process is due.

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?

A: Just reiterating what I said at the hearing, I do not believe that Board has the power to make "declarations" about the constitutionality of any Presidential action.

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?

A: I generally agree, but it is not possible for me – and I suspect that it would be impossible for anyone - to draw a general or comprehensive line between which national security matters require judicial process and which ones do not. In some areas, the line is well-established: For example, security clearance determinations are not subject to judicial process.

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?

A: I am not sure whether the killing of al Awlaki is a matter upon which the Board should focus its limited resources. Before forming an opinion on that, I would want to hear the views of relevant Executive branch officials, as well as of Members of this and other committees that have an interest in the matter. If the Board were to take up the matter, and if I were confirmed as a member of the Board, I would expect the Board to request a copy of the legal reasoning used to justify the killing. Regardless of the role of the Board, I support Congress having a copy of that opinion. Generally, I believe that the Executive Branch's legal reasoning regarding its powers should be made public, with appropriate security redactions.

(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?

A: 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?

A: The Board will have limited resources, and, if confirmed, I will work with the Chairman and the other members of the Board to ensure that they are wisely spent. If confirmed, I would urge that the Board consider a full range of cost-effective possibilities, including occupying secure space previously used by another entity, if any becomes available, or to co-locate in a facility where the security costs would be reduced.

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

A: I expect that a large percentage of the work of the Board will require access to classified information or discussion with officials about matters that are classified.

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?

A: The statute establishing the Board requires it to prepare, at least twice a year, a report "which shall be in unclassified form to the greatest extent possible." In addition, the statute specifies that the Board "shall— (1) make its reports, including its reports to Congress, available to the public to the greatest extent that is consistent with the protection of classified information and applicable law; and (2) hold public hearings and otherwise inform the public of its activities, as appropriate and in a manner consistent with the protection of classified information and applicable law." It is my assumption, however, that the Board will not have the ability to publish any previously classified information without the approval of the Executive Branch. I expect that, like other oversight bodies, the Board would engage in discussions with the Executive Branch about what could and could not be published.

(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?

A: As you describe, U.S person is defined in FISA.

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?

A: I have not studied this question, but based on what I know now, I do not believe that the definition of U.S. person should be broader.

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

A: Already, the concept of U.S. person causes problems for quickly sharing terrorism information, so expanding the definition would logically expand the problem.

(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?

A: There is no express authority for the Board to file amicus briefs, and I do not believe that the filing of amicus briefs would be a wise 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?

A: I do not support recreating the wall as part of cybersecurity legislation. One aspect of the wall pre-9/11 was that information collected under surveillance statutes – in compliance with applicable rules for judicial authorization - for counter-terrorism purposes could not be shared with and used by other units *for counter-terrorism purposes* if the units were operating under different legal categories (law enforcement vs. intelligence). For example, FBI agents conducting the criminal investigation of the African embassy bombings by al Qaeda were prohibited from sharing the information they obtained under the powers of the grand jury with FBI agents investigating al Qaeda under the FBI's foreign counter-intelligence authorities, while FBI agents conducting court-ordered FISA surveillance of terrorism targets in the US were prohibited from sharing that information with FBI agents conducting criminal investigations of the same group. By bringing down the wall, Congress ensured that all counter-terrorism information could be shared with all counter-terrorism agencies. The issue currently under discussion in the context of cybersecurity legislation is in some ways different: Should information collected for cybersecurity purposes be used by non-cybersecurity agencies for non-cybersecurity purposes? In particular, should information collected "notwithstanding any other law," including the content of domestic communications collected inside the US without a court order, be shared with agencies not involved in cybersecurity and used for other purposes unrelated to cybersecurity? I believe that a balanced solution to that question can be achieved.

(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?

A: I believe that information obtained obtained by the government from the private sector without a court order for cybersecurity purposes should be able to be shared with law enforcement to be used for investigating and prosecuting cybersecurity crimes. For example, if a private company uncovers information indicating that a person has hacked into the company's network in an effort to steal its intellectual property, the company should be able to share information about this cyber attack with other companies and with the federal government to help prevent such attacks on others, and the information shared could be used to investigate and prosecute both a violation of the Computer Fraud and Abuse Act as well as attempted theft.

(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?

A: Yes.

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?

A: As I said at the hearing, I would, if confirmed, work in my capacity as a member of the Board within whatever structure Congress enacts. I have argued that information shared for cybersecurity purposes should generally be used only for cybersecurity purposes, including for the investigation and prosecution of cybercrimes and crimes committed by cyber means and for national security purposes related to cyber (such as responding with other appropriate foreign policy, intelligence and national security options to China's efforts to steal government and commercial data). S. 2105, the Cybersecurity Act, introduced by Senators Lieberman and Collins, would place some reasonable limits on the use of information that is shared with the federal government for cybersecurity purposes. In addition, all of the leading cybersecurity bills limit or prohibit the use of cybersecurity information for regulatory purposes. Placing limits on the use of information shared for cybersecurity purposes could help make the information sharing program a success. Under all pending cybersecurity legislation, information sharing would be voluntary. ISPs and others would share very little or they would share useful information based on their perception – and their customers' perceptions – of how the information is being used. Companies might be more willing to share, and the national cybersecurity posture would be improved, if companies and their customers were assured that information was not being used broadly for non-cybersecurity purposes. A failure to specify how the information may be used could make it less likely that companies would voluntarily share in the first place.

I believe that information shared with the government under a cybersecurity exception may properly include the content of communications, since it is often the content that constitutes the malicious code or the attack signature.

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?

A: Please see my response to question #2, above. Additionally, in terms of the minimization or redaction of PII, there should only be, at most, redaction of non-relevant PII. Some PII will be directly relevant to the utility of the information for permitted purposes.

4. How long should any shared information be retained?

A: Retention should be based on the utility of the information for cybersecurity purposes and for other permitted uses that have been identified.

(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.

A: Justice Sotomayor's discussion of the length of time that monitoring occurred was quite limited, and the question essentially quotes all of the relevant text: Justice Sotomayor was agreeing with Justice Alito that, "at the very least, 'longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy,'" and she went on to say that in cases involving "short-term monitoring, some unique aspects of GPS surveillance relevant to the *Katz* analysis will require particular attention." I agree with Justice Sotomayor both in her reading of Justice Alito's opinion and in her statement that, in determining what is a "search" under *Katz's* reasonable expectation of privacy test, the unique attributes of GPS surveillance merit attention.

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?

A: I do not believe that is possible to say in the abstract whether the Fourth Amendment has a temporal restriction. Time may have some relevance to determining whether a search or seizure is reasonable. See *Terry v. Ohio*. In addition, in *Jones*, Justice Alito said that time was relevant to determining whether a search had occurred: "relatively short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable. See *Knotts*, 460 U.S., at 281-282. But the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy."

(13) Agency Authority

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?

A: The statute creating the Board states that the Board "shall … analyze and review actions the executive branch takes to protect the Nation from terrorism." It also states that the Board "shall continually review … the procedures, and the implementation of the regulations, policies, and procedures, of the departments, agencies, and elements of the executive branch relating to efforts to protect the Nation from terrorism to ensure that privacy and civil liberties are protected."

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?

A: To the extent that the Vice President and the Office of the Vice President are involved in actions that are "actions taken by the executive branch," please see my response to question A, above.

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

A: In the situation you describe, the Board is required to act under subsection (e)(2)(D) of the stature establishing the Board. If confirmed, and if confronted with such a situation, I would urge the Board to fulfill that requirement with the utmost care and discretion.

C. 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?

A: I think the term means that the President and other members of the Executive Branch cannot control the reports of the Board or direct its activities. I have not studied the authority of other, fully independent boards outside the Executive Branch.

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?

A: The statute establishing the Board provides that, whenever information or assistance requested is, in the judgment of the Board, unreasonably refused or not provided, the Board shall report the circumstances to the head of the department, agency, or element concerned without delay, and the head of the department, agency, or element concerned shall ensure that the Board is given access to the information, assistance, material, or personnel the Board determines to be necessary to carry out its functions. Such a report to the Attorney General would probably be something that the Board would be required to describe to Congress as a "major activity" in its semi-annual report to Congress.

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?

A: I think it would be more likely for the Board to report the situation to Congress.

(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?

A: If confirmed, as sources of law for evaluating the legality and propriety of U.S. government actions to fight terrorism, I will rely exclusively on the requirements of the U.S. Constitution, as interpreted by the Supreme Court, and on U.S. law, including treaties to which the U.S. is a party and other international law to which the U.S. is subject and not on foreign countries' laws or on allegations of what international law requires.

Questions for the Record – Responses of James X. Dempsey

Questions from Senator Klobuchar

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?

A: For the past 27 years, my career has focused specifically on the need to balance civil liberties with national security and other priorities.

From 1985-1995, I was Assistant Counsel to the House Judiciary Subcommittee on Civil and Constitutional Rights, working on issues involving national security, law enforcement, government surveillance, death penalty procedures, and government databases and information systems, among others. During that period, one example of balancing civil liberties with national security and law enforcement interests was my work as a Congressional staffer in connection with legislation that became the Communications Assistance for Law Enforcement Act of 1994. In the early 1990s, the FBI brought to the attention of Congress concerns that its ability to carry out electronic surveillance was being eroded by factors associated with the transition to digital technology in the nation's telephone networks, the growing importance of mobile telephone, and other technological developments. The FBI urged Congress to adopt legislation requiring telecommunications service providers to design their networks to ensure that the government could readily tap them. The issue presented a need to balance three interests: the government's interest in being able to expeditiously conduct electronic surveillance in criminal and national security investigations, the interests of industry in being able to continue to innovate and offer new features and services, and the values associated with privacy. Working on behalf of the Chairman of the Subcommittee on Civil and Constitutional Rights, I developed and managed a process of consultation with all affected stakeholders. In this effort, I coordinated with minority counsel for the Subcommittee and with staff for the Senate Judiciary Committee. We met multiple times with officials of the FBI, the telecommunications industry, academic experts in network operations and security, and privacy advocates. We convened a series of consultations bringing the parties together for dialogue, seeking to develop a better understanding of the technology, of law enforcement's needs, and of the implications for innovation and privacy. The resulting legislation, CALEA, passed the House on suspension in 1994.

Another example of my work balancing civil liberties and national security was my participation on the Markle Foundation's Task Force on National Security in the Information Age. After the attacks of 9/11, and after it became clear that the failure to share information contributed to the government's failure to identify and prevent the plot, the Markle Foundation convened a bi-partisan task force of former government officials, business leaders, technologists and civil

liberties advocates. I was privileged to serve first as participant in the task force's discussions, then as a member of the Task Force, and then as member of the Task Force steering group. The Task Force met over the course of 4 years, producing a series of reports that influenced and are reflected in the report of the 9/11 Commission, an executive order issued by President Bush, section 1016 of the ITRPA, the amendments to section 1016 in the 9/11 Commission Act, and ICD 501. In the course of that work, we met with officials of the NCTC, NSC, DHS, and FBI. We drew on the expertise of technology experts. The members of the Task Force engaged in extensive dialogue with each other, achieving the consensus reflected in the Task Force's reports and other work products.

Another example of seeking to balance civil liberties with national security was my work as a member of the TSA's Secure Flight Working Group, convened by the Transportation Security Administration in 2005. The small group of technology and privacy experts met with officials of the TSA responsible for passenger screening, reviewed documents relating to the development of Secure Flight, and engaged in extensive dialogue to develop a consensus report, which recommended a program very similar to that which was ultimately adopted by TSA.

Also in 2005, I was privileged to be a member of a bi-partisan group of former government officials who developed recommendations regarding the expiring provisions of the PATRIOT Act. The group included a retired 4 star general, a former deputy secretary of Homeland Security and a former White House chief of staff, as well as the current Attorney General and the current general counsel of the NCTC. The group met over a period of months and developed consensus recommendations for improving the expiring provisions of the Patriot Act.

More recently, in a related area, I worked on balancing privacy with the important energy management goals associated with the Smart Grid. In 2009, the California Public Utilities Commission commenced a set of proceedings designed to adopt rules to encourage deployment of the Smart Grid. I was intensively engaged in the proceedings. I met with other consumer advocates, with the utilities, and with companies developing Smart Grid technology. Working collaboratively with other privacy advocates, I helped lay out a comprehensive data privacy framework, which the PUC adopted. Based on that framework, I then helped draft a detailed privacy rule intended to provide both the clarity and the flexibility demanded of this still evolving field. Most importantly for purposes of your question, I worked with Pacific Gas & Electric to develop the proposed rule, which was presented to the PUC as a joint privacy-PG&E proposal. After extensive comment and some revisions, the PUC adopted a privacy and security rule based largely on the proposal I had helped craft.

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?

A: This is an important question, although, in my view, privacy concerns in the commercial arena are largely not within the jurisdiction of the PCLOB.

The dynamics of privacy are very different in commercial contexts as opposed to security contexts because the interests in the use of the data are very different. The rules that would be applicable in the commercial context are not the same as those that would be applicable in the commercial context. Nevertheless, the framework for identifying and addressing privacy questions is roughly the same, as the Department of Homeland Security explained in its 2008 Privacy Policy Guidance Memorandum.

I believe that industry, including telecommunications firms, and the government can work together to improve our approach to privacy issues. Already, advertising networks and browser developers are working together with consumer advocates and the government to implement Do Not Track (DNT) technology that makes it easier for users to control online tracking. One forum for cooperation where DNT is being developed is in the World Wide Web Consortium (W3C), where privacy advocates and companies are working together to develop the technical standard that will be used to implement DNT. Another example of industry-government-consumer cooperation is the Botnet Working Group, where industry, government and consumer advocates are working together to develop best practices for ISPs in responding to the botnet infection of their customers' computers, a problem that poses a serious risk to both privacy and security.