WHITE HOUSE PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD

Georgetown University

Washington, D.C.

Professor Arend: Ladies and gentlemen, I want to welcome you to Georgetown University and encourage you to move up towards the front if that is indeed possible. My name is Anthony Arend with my colleague, Chris Joiner, I direct the Institute for International Law and Politics here at Georgetown and it is a great honor to have here today the first public meeting of the White House Privacy and Civil Liberties Oversight Board.

As many of you know, this Board was recommended by the 9/11 Commission and was ultimately established by the Intelligence Reform Act of 2004. I'm going to let the distinguished Chair and Vice-Chair talk more about the specific goals and purposes of the Board but I would like to introduce the Board members before we have our first panel.

I should note, the Intelligence Reform Act requires Board members to be appointed from among trustworthy and distinguished citizens outside the federal government who are qualified on the basis of achievement, experience and independence and the Board members we have here this afternoon clearly

recognize and represent those qualities.

The Chair of the Board is Ms. Carol Dinkins. She is a Partner with Vinson and Elkins, where she chairs the Administrative and Environment Law Section. She did her B.A. degree at the University of Texas at Austin and her law degree from the University of Houston Law Center. She was appointed Assistant Attorney General in charge of Environment and Natural Resources Division in the Justice Department in 1981. In 1984, she was appointed the Deputy Attorney General of the United States. She served as an officer and briefly as Chair of the Board of Directors of the Nature Conservancy, as many of you know, an international conservation organization. From 2002 to 2003, she chaired the ABA Standing Committee on the Federal Judiciary. This is the committee that vets and recommends all individuals nominated for Article III Courts.

The Vice-Chair of the Committee is Mr. Alan Raul. He is a Partner in the Washington, D.C. law firm of Sidley and Austin. He has a broad litigation and counseling practice covering

administrative law, government regulation and enforcement, corporate compliance, as well as privacy and information law. He did his undergraduate degree at Harvard College. He has a Masters from the Kennedy School of Government at Harvard and then he went to Yale Law School to receive his J.D. He cleared for Judge Malcolm Wilkey on the D.C. Circuit Court of Appeals and he has served as General Counsel in the Office of Management and Budget from 1988 to ’89 and General Counsel of the U.S. Department of Agriculture from 1989 to 1993. He has written widely in areas of concern to the Board, including a recent book entitled, Privacy and the Digital State, balancing public information and personal privacy.

Next we’ll turn to Mr. Lanny Davis. Mr. Davis is a Partner in the Washington firm of Orrick, Harrington and Sutcliffe, where he is a member of the Litigation Practice Group. From 1996 to 1998, Mr. Davis served as a Special Counsel to the President at the White House and was spokesperson for the President on matters concerning campaign

finance investigations and numerous other legal issues. He did his undergraduate work at Yale College and went on to go to the Yale Law School, where he served on the Yale Law Journal. At Orrick, Harrington and Sutcliffe, he manages a unique legal crisis communications practice. He has been featured, as many of you know, in articles in U.S.A. Today, Forbes, Fortune Magazine and a variety of other publications.

Now turn to Theodore Olson. Ted Olson is a Partner in Gibson, Dunn, Crutchers' Washington, D.C. office. He is Co-Chair of the Appellate and Constitutional Law Practice Group as well as the firm's Crisis Management Team. As I suspect everyone knows, he was a distinguished Solicitor General of the United States from 2001 to 2004. Prior to that, he had also served in the Justice Department as Assistant Attorney General in charge of the Office of Legal Counsel.

As everyone knows, he is one of the nation's premiere advocates. He has argued 43 cases before the U.S. Supreme Court and according to my notes,

has won 75 percent of those cases, so he has a distinguished record.

Our final Board member is General Francis Taylor. He was recently appointed the Chief Security Officer for the General Electric Company in March 2005. In that job, he is responsible for overseeing GE's global security operations and crisis management processes. Prior to joining GE, General Taylor had a distinguished 35-year career in government service, where he held numerous senior staff positions. Most recently, he was the Assistant Secretary of State for Diplomatic Security and Director of the Office of Foreign Missions, which he held with the rank of Ambassador. General Taylor also served as the U.S. Ambassador at Large and Coordinator for Counter-Terrorism for the Department of State, from July 2001 to November 2002. During his 31 years of military service, General Taylor served with distinction many military command and staff positions, rising to the rank of Brigadier General. He has received numerous awards, including the Distinguished Service Medal, the

National Intelligence Distinguished Service Medal, the Legion of Merit and the Department of State Distinguished Honor Award. He did both his Bachelor's degree and his Masters degree at Notre Dame University.

So ladies and gentlemen, we want to again welcome the Board and I will turn it over to Ms. Dinkins.

Ms. Dinkins: Thank you, Professor Arend, for those kind opening remarks and that introduction. Good afternoon on behalf of the Privacy and Civil Liberties Oversight Board. I want to welcome our panel members and our Privacy Officers to Georgetown University and thank you for making time in your schedule to be here with us this afternoon.

As we work on our continuing efforts to identify and to prioritize policies, programs and issues that warrant our attention. We look forward to hearing of your interests and concerns.

Let me thank University President, John DeJoria and the staff of the Office of Protocol and Events for making this extraordinary venue available for us

and for their logistical support over the past month.

The Board is appreciative of those in the audience, for your interest in the Board and its activities. This is a particularly busy time for the University community. All of us recognize what a busy time it is and we thank the students, the professors and the administrators who show their interest in the Board by attending today's meeting.

This is the Board's first public meeting and it is designed for us to hear from a wide range of individuals and organizations with special interests and expertise in privacy rights and in civil liberties, specifically in the context of protecting the nation against terrorism. It is the latest in a series of meetings that we've had with prominent public policy organizations, academia, and private advocacy groups.

The creation of this Board was recommended by the report of the 9/11 Commission and it is authorized by the Intelligence Reform and Terrorism Prevention Act of 2004. Vice Chairman Alan Raul and

I were confirmed by the Senate on February 17 of this year and we were sworn into office, along with our colleagues, Lanny Davis, Ted Olson and Frank Taylor at our first meeting on March 14 of this year.

Our activities and our efforts since then have been dedicated to the necessary administrative, introductory and educational elements of establishing, as they say in Washington, standing up a new institution. We've met regularly with senior White House staff and with Administration officials with whom we work closely. We have visited most of the major departments and the agencies charged with protecting the nation against terrorism. We are integrating the Board into the relevant policy development and implementation processes that exist within the Executive Branch and we've successfully accomplished a number of basic administrative matters, such as building out space, hiring a staff and getting the necessary security clearances into place.

The Board is very pleased with the level of

support that we have received from the Administration on all these efforts.

But our most important accomplishment to date has been to focus our attention on the issues we believe we can provide the greatest service to the American people and to fulfill our statutory responsibilities.

Vice-Chair Alan Raul will talk more about this but please know that all of our efforts have been undertaken as a group. The members of the Board share a unanimity of purpose and dedication to carrying out our responsibilities.

Please be assured that this is not a stand-alone event. This meeting is the beginning of what we expect to be an on-going discussion. You should always feel free to raise your comments, your concerns and maybe even an occasional compliment.

With that, I'll pass the mic to Vice Chairman Raul.

Mr. Raul: Thank you, Carol. In addition to those who you've already thanked for making today's meeting possible, I would like to acknowledge and

thank two of our colleagues from the Privacy and Civil Liberties community, from within the Executive Branch, who have been able to join us here this afternoon. Alex Joel is the Civil Liberties Protection Office from the Office of the Director of National Intelligence and Jane Horvath is the Chief Privacy and Civil Liberties Officer at the Department of Justice. Thank you for being here.

The Board views its mission of providing advice and oversight with regard to privacy and civil liberties as benefiting from and drawing on the government's substantial existing resources and efforts in this area. We therefore greatly appreciate the ongoing help and support we receive from these and other representatives of the government's Privacy and Civil Liberties or PCL community.

Moreover, the Board places a very important priority on assisting these Privacy and Civil Liberties Officers in carrying out their work within their own agencies.

As Carol noted, the Intelligence Reform and

Terrorism Prevention Act of 2004 charged the Board to carry out broad responsibilities. Our statutory mandate includes providing advice and oversight on the Privacy and Civil Liberties issues implicated in both the development and the implementation of anti-terrorism policies.

We have had, to date, good access to the most sensitive information about how those policies are being implemented. So far, we have seen that senior officials, lawyers, inspectors general and program operators seem to be highly sensitive about they handle and protect the information they target, acquire and retain about U.S. persons.

Besides our review of policy implementation, there are also, in my view, at least two other core dimensions to the Board's work. One is how deeply the Board can participate within the Executive Branch in advising on the development of counter-terrorism policies and second, is how much information the Board can share with the public about the protections incorporated into both the development and implementation of those policies.

On the public side, I believe the Board can help advance both the interests of national security and the rights of Americans by helping explain how the government safeguards U.S. person information.

In short, we hope that the Board's efforts to provide additional public explanation of the government's internal checks and balances, could be a win-win for both the warriors against terrorism and the advocates for civil liberties.

With regard to the Board's substantive priorities, we are statutorily obligated to be consulted and provide advice regarding the new Information Sharing or ISE Guidelines. The Board's staff has participated extensively in the policy coordinating committee, jointly chaired by the National Security Council and the Homeland Security Council staff and we are currently working with the ISE Program Manager on a format for continued oversight.

Other areas of focus include government surveillance programs, data mining, and government use of commercial data, the Patriot Act and other

domestic intelligence gathering issues. And the Board has also become deeply involved in questions surrounding anti-terrorist no-fly and other watch lists and related screening issues. We're working closely with an interagency group to enhance the quality of the anti-terrorist Watch List themselves, which would immediately reduce false positives and also to improve the mechanisms for individuals to obtain redress when they believe they have been wrongly listed or screened.

We hope to be able to encourage very tangible progress in this area, a subject that impacts the daily lives of Americans and travelers to and from the United States.

The last point I will mention concerns the so-called U.S. Person guidelines, issued by the Attorney General for each intelligence agency under Executive Order 12333. These are very detailed sets of mandated protective measures for the treatment of intelligence information about or referring to American citizens and residents. The Board plans to work with the Director of National Intelligence and

the Department of Justice to promote clarity and consistency in these guidelines, as called for in the March 2005 Weapons of Mass Destruction report. The existence and impact of these highly protective guidelines is not particularly well understood by the public and we believe that streamlining and explaining them better would be useful, both inside and outside the government.

This discussion of Board priorities is intended as an illustration of the issues we are examining. The purpose of this meeting is to help develop the Board's thinking on our established priorities as well as identifying additional issues and information that may warrant our attention.

We look forward to a continuing dialogue with the Privacy community and all parties interested in promoting consideration of privacy and civil liberties.

So again, on behalf of Chairman Dinkins, myself, and all Board members, thank you very much for helping us advance our important and challenging mission.

Ms. Dinkins: Thank you. We will now hear from Board Member Lanny Davis, who will also introduce the first panel.

Mr. Davis: Good afternoon and thank you all for being here. Before I have the privilege of introducing this panel, I did want to make one very brief opening comment and it's appropriate that I am introducing this panel because of what I would like to say.

I was raised in a household where the ACLU was a heroic organization and I still believe it to be so. I was raised by parents who valued civil liberties and privacy rights in an era where political views sometimes led to blacklists and to ruined reputations and lives.

So, post 9/11, when I received the honor and privilege of being invited by President Bush to serve on this Board. I said yes, still with the background in presumption that civil liberties and privacy rights can be reconciled with the imperative of protecting our country from murdering terrorists and from people who don't care about taking innocent

lives.

Our chief burden as a Board is to find the right balance between my own and I believe, my colleagues, commitment to civil liberties and privacy rights, while still giving our government the ability to protect our country, our children and all of us, from these forces of evil that we all saw and experienced on 9/11.

So with that as an introduction, I would like to introduce our panel very briefly. Why don't we do it one at a time and then I'll introduce each of you after you've finished your remarks.

So first, is it Caroline or Carolyn? Caroline. I'm married to a Carolyn so – Caroline Fredrickson, Director of the Washington Legislative Office of the American Civil Liberties Union and I won't go through everybody's full biography except the one I like most in Caroline's is that she is a Summa Cum Laude graduate from one of the great universities in the universe, Yale University.

Ms. Caroline Fredrickson: Thank you very much. It's really an honor to be here and I appreciate

your having us, the ACLU, to testify today. As Mr. Davis mentioned, I am Caroline Fredrickson. I am the Director of the American Civil Liberties Union's Washington Legislative Office.

This hearing is a welcome but unfortunately long overdue first step to air just some of the civil liberties transgressions of this Administration over the past five years.

So much has changed in America since 9/11. Regrettably, our privacy and civil liberties suffered significant collateral damage in the subsequent War on Terror. Americans have begun to piece together this puzzle and we're asking, why does the President think we're the enemy in the War on Terror?

Here are the violations of civil liberties that most concern the ALCU.

Warrant-less wiretapping and consumer call information. In violation of federal law and the U.S. Constitution, the National Security Agency is listening, without a warrant, to telephone calls of Americans who are in the United States, who are

talking to people abroad.

In August 2006, a federal judge in Detroit found the eavesdropping program both unconstitutional and illegal as a result of an ACLU lawsuit.

The NSA is also scanning phone records turned over by telecommunications companies in violation of state statutes and regulations. The NSA has gained direct access to the telecommunications infrastructure through the willing cooperation of some of America's largest phone companies. The NSA also appears to be using broad data mining systems that allow it to analyze information about millions of innocent people in the United States without clear legal authority to do so and at the cost of American's privacy.

Torture, kidnapping, and detention. The government continues to claim that it has the power to designate anyone, including Americans, as enemy combatants without charge. Investigations into detention centers have revealed severe human rights abuses and violations of international law in the

Geneva Conventions. The government has also engaged in the practice of rendition, secretly kidnapping people and moving them to foreign countries where they are tortured and abused. Last week, ALCU client Khalid El-Masri traveled from his home in Germany to Washington, D.C. to describe his appalling experience of being abducted and tortured for months. El-Masri is our client in the ACLU's landmark lawsuit charging former CIA Director George Tenet, other CIA officials and U.S.-based aviation companies with violations of U.S. and universal human rights laws.

The U.S. government sponsored torture of the past several years is a shameful chapter in American history.

Government secrecy. The Bush Administration has weakened the Freedom of Information Act through willful noncompliance and has engaged in a campaign of reclassification and increased secrecy, including the expansion of a catch-all category, called Sensitive but Unclassified and has made sweeping claims of state secrets to stymie judicial review of

its policies that erode civil liberties.

Until recently, it even refused to grant administration investigators the security clearances they needed to investigate the illegal and unconstitutional NSA wiretapping program and this Board had to wait 11 months to be even partially briefed on some aspects of a program that the public learned about from the New York Times, almost one year ago. And yet, the Administration wants to prosecute journalists under the Espionage Act of 1917, to thwart the media's role in exposing such questionable and illegal conduct.

Real ID. The Real ID Act leaves the foundation for a national ID card. Under the law, states must standardize drivers' licenses and link to data bases shared with every federal, state and local government official in every other state. The aggregation of our private information into a massive database would create one-stop shopping -- for identity thieves. Yet defying all logic, the Department of Homeland Security refuses to build privacy protections into the database, the ID card

or the data transmission systems because the Act fails to mention the word, privacy.

No-Fly Lists. These were established to track dangerous people the government prohibits from traveling. Since 9/11, the number of watch lists has mushroomed, all with subjective or inconclusive criteria for placing names on the lists and with little or no means to remove them. These lists name an estimated 30 to 50 thousand people and are so erroneous that several members of Congress, including Senator Ted Kennedy, have been on them.

Political spying. Government agencies such as the FBI and the Department of Defense, spied on innocent, law-abiding Americans. The ACLU learned through the Freedom of Information Act, that the FBI has consistently monitored peaceful groups, such as the Quakers, People for the Ethical Treatment of Animals, Green Peace, the American Arab Anti-Discrimination Committee and of course, the ACLU.

Abuse of the Material Witness statute -- following 9/11, the government detained many people in the United States, mostly Muslims, by exploiting

a provision that permits the arrest and brief detention of material witnesses or those possessing important information about a crime. Most of those detained, however, were never treated as witnesses to crimes of 9/11 and some were imprisoned for more than six months and one actually spent more than a year behind bars.

I'm not going to spend a lot of time on the Patriot Act because I think people know where the ACLU stands on that legislation.

But let me say, all is not well. When our government is torturing people and spying on Americans without a warrant, this Board should act! Indeed, should have acted long ago. Clearly, you've been fiddling while Rome burns. Your claimed 17 meetings consist mainly of phone calls or teleconferences with administration insiders. This is the first public meeting you have had.

The PCLOB should begin aggressive investigation into several important matters. First, the Board should review the policies and procedures by which the NSA or other federal agencies intercept

communications where there is no probable cause to believe the people targeted are either agents of a foreign power or criminals. This is the most pubic dispute over the intersection of new anti-terror efforts and civil liberties and privacy principles so vital to our way of life.

Some of you have been recently quoted as saying that your review of this wireless wiretapping gave you greater confidence that protections were built in. Yet it is clear that this program violates the Foreign Intelligence Surveillance Act and the Fourth Amendment. You can put lipstick on a pig but it's still a pig.

Second, the Board should use its authority to conduct public hearings and issue regular, public reports that explain its findings. Doing both will heighten public and government awareness of the importance of vigorously protecting privacy and civil liberties.

Third, the Board should review the vast implications posed by watch lists. Certainly it is useful for the government to maintain a list of

people who are known to be dedicated to committing violent acts against America but the utility of the current list is so limited, especially because it's hard for innocent people to get off and stay off these lists.

Congress never established any legal criteria for placing people on any list and no court has ever squarely decided the constitutionality of using such lists to deny the exercise of certain rights and privileges, nor has any body fully reviewed how names are shared between agencies or the implications of such sharing. Thus, the result is wholly unregulated, threatens due process and impedes the exercise of First Amendment rights of petition of redress -- the right to travel and it may prevent individuals from even entering government buildings to obtain services.

Finally, the Board should investigate the government's contracting with private companies to perform quasi governmental roles. In particular, the investigation should focus on those companies facilitating voice and data communications

interception -- data mining analysis and background and clearance searches on potential government employees. For example, data aggregator Choice Point has many government contracts for most federal anti-terror and anti-crime agencies. Yet its data is notoriously rife with errors, including the well-documented merging of files of several individuals with similar names.

But this Board lacks any power to effect those changes. It's all bark and no bite. While the Board may access information and documents from an Executive Branch agency or department. It may interview officers of other agencies and request information from state, tribal or local governments. It does not have subpoena power. So it can't necessarily get any of that information.

And it lacks independence, slotted as it is in the Executive Office of the President. Contrary to its name, the Board has little, if any, oversight authority. Representatives Ms. Carolyn Maloney, Chris Shays and Tom Udall have introduced legislation, which would take the Civil Liberties

Board out from under the President's control and would it give it subpoena powers. We strongly support that necessary move to ensure that the Board has true oversight powers.

Last week, the ACLU represented Khalid El-Masri, a German citizen who was kidnapped by our government, thrown into a secret prison and tortured. I wish the members of this Board had been able to look Mr. El-Masri in the eye as I did and hear his firsthand account of this dark chapter in American history.

History has shown that a nation that compromises freedom unnecessarily compromised its most precious values and history will show that this Administration has been on the wrong side of civil liberties. We can be both safe and free.

The ACLU and its members urge you to undertake the review of the pressing matters I've addressed today and then make your findings and recommendations known not only to the President and Executive Branch but also to the people. Thank you.

Mr. Davis: Thank you very much, Caroline.

Excellent and moving statement. I would like to introduce David Keene of the American Conservative Union. David is a graduate of the University of Wisconsin Law School and has been a John F. Kennedy Fellow at Harvard University's Institute of Politics. There you have - I said the name, Harvard, David, even though it's hard.

Mr. Keene: It's tough.

Mr. Davis: Tough. And also a First Amendment Fellow at Vanderbilt University's Freedom Forum. David?

Mr. David Keene: Thank you. Let me begin by thanking you for the opportunity to address the Board this afternoon. I am Chairman of the American Conservative Union, attorney, a writer and Co-Chair with David Cole of this University of the Constitution Projects Bipartisan Liberty and Security Initiative.

Many conservatives have been concerned since 9/11 that in reacting to the very real dangers posed by international terrorist networks. Those within our government charged with safeguarding our

security, might take action that could significantly alter the very nature of the free society they are working to protect.

History teaches us that in times of international crisis, Americans are often more than willing to trade a measure of their freedom for increased safety and security and that government has all too often been willing to broker the trade. From the Civil War to World Wars I and II, to Vietnam and now the War on Terror, conscientious but overzealous government officials have sought as power as they could get to make it easier to protect us. In many cases, they were given or assumed too much power or used that which they were given without the care one might reasonably expect from men and women charged not simply with protecting U.S. real estate but also with safeguarding the way of life that makes our nation unique.

In virtually all cases, those granting these powers and those exercising them were acting in good faith. When Abraham Lincoln suspended habeas corpus rights during the American Civil War, when Woodrow

Wilson sought the power to quash what he saw as disloyal opposition to this nation's role in World War I, when Franklin D. Roosevelt authorized the internment of Japanese, German and Italian Americans during the Second World War, and when Richard Nixon sought intelligence on those he and his Administration believed to be domestic terrorists, they did so because each believed he was acting responsibly to protect the nation he had sworn to defend.

Despite their detractors, none of these men were motivated by desire to weaken the constitution or undermine the freedoms they were sworn to uphold. On the contrary, each of them acted because he believed the actions he took were essential to the protection of those freedoms and therefore, entirely consistent with the oath he had taken. But that did not make them right.

Today, Congress and the Bush Administration have combined, for the same reasons, to give the Executive Branch new powers to investigate, identify, apprehend and prosecute potential

terrorists. Much of what they have sought and been granted deserves our support. 9/11 caught this country flat-footed and it became instantly clear to all that dealing with this new threat would require new tools to allow coordination and information sharing among intelligence and law enforcement agencies and to make certain that laws developed decades ago were updated to meet the needs and threats of today.

However, the atmosphere in which initial decisions were made was, to be charitable, less than conducive to sound decision-making. Since then, there have been limited reforms and some sweeping proposals or plans have been dropped. We can all remember the uproar over CAPS II passenger screening proposals a few years ago that forced the government to back to the drawing board and Operation TIPS that was scuttled by the Congress or the controversy over the total Information Awareness Program.

But controversy still surrounds other programs initiated since that time. The Washington Post, among others, has reported that members of this

Board were recently briefed on the NSA Program so I'd like to emphasize our view that we have never believed that the issue is whether the government can or should, under certain circumstances, conduct such surveillance but whether such activities should be conducted in compliance with our constitution and existing law.

It is our hope that this Board will provide critical oversight of such programs and ask the hard questions of those running them that you are in a unique position to ask. A President's good intentions do not put him above the law. We continue to be troubled by the argument that a President has no obligation, because of the Inherent Powers Doctrine, to follow the law or respect other constitutional guarantees whenever he evokes national security as a justification for his actions.

In the context of electronic surveillance, the fact is that the Congress provided the President the authority to conduct these activities subject to reasonable restrictions and oversight. The simple

assertion that such restrictions and oversight make it impossible for the government to do an effective job, can never be accepted alone as justification for flaunting or ignoring existing law.

To more fully explain why the existing NSA Surveillance Program does not comply with these legal requirements, I am submitting today a copy of a Friend of the Court brief that the Constitution Project and the Center for National Security Studies filed last month in the U.S. Court of Appeals for the Sixth Circuit. I urge this Board to review the NSA Program carefully and take advantage of your position to make recommendations for bringing this program into compliance with the rule of law.

We're pleased that this Board is playing a role in an attempt to reform the way in which watch lists are complied and used. The Constitution Project is also releasing today a statement on processes we believe ought to be adopted with reference to the utilization and potential abuses of so-called watch lists. A copy of that statement is available here.

We believe strongly that the use of such lists

should be strictly limited to circumstances like airport screenings, where for time reasons, more thorough checks can't be completed and grave consequences might follow from a failure to screen out a listed person. By contrast, we believe that such lists should not be used to screen people for purposes of employment.

In addition, we recommend procedures to provide for improved accuracy in creating watch lists and to allow people wrongly included on such lists to get their names removed. The way in which such lists are thrown together today and the hardships experienced by innocent travelers as a result, have become something of a national scandal. We can certainly do better.

When the Patriot Act was reauthorized by the current Congress, the reauthorization included some needed reforms. But many of us are fearful of programs that put more and more investigative power into the hands of federal law enforcement officials without making those powers the focus of continual oversight and court review. We've been fortunate

thus far, I think, in that while there have been some abuses, the Justice Department has yet to push the edge of the envelope, so to speak, with the new tools available to it. But history again tells us that the day will come when that happens.

In one sense, it is already happening. The initial reason behind the request for additional powers was the need to thwart terrorists with designs on doing harm to this nation and her citizens. We were told that the nature of the struggle in which we find ourselves and the technological advances of recent decades required that government have the power to gather information and act on it quickly, often without paying much attention to the safeguards envisioned by the constitution.

It’s not difficult to envision scenarios in which this is both obvious and true. If investigators came upon credible evidence that terrorists might, for example, have a nuclear, biological or chemical weapon in place and ready to go off in one of our cities, we might want them to

move quickly to locate it and prevent its detonation without requiring them to observe the legal and constitutional niceties that we would expect of them in say, a tax evasion investigation. But the need for exceptions for so-called exigent circumstances cannot be permitted to expand much beyond the very immediate ticking time bomb period.

Unfortunately, our efforts to combat terrorism are likely to continue for the foreseeable future. It's even more critical, in such a sustained period of enhanced security, that we also safeguard our constitutional freedoms and preserve the Rule of Law.

What we believe is required is a sense of proportion in reviewing the operation of laws impacting constitutional rights and effecting the traditional rights of privacy that U.S. citizens have come to consider a part of their birthright. We cannot expect that sense of proportion to come from those utilizing these new powers granted to them, for their mission requires them to utilize all the tools available to protect us. They cannot,

themselves, be the ones who establish the ground rules or cry foul when they are broken. That's the role of Congress, through its oversight function, the courts, the media and importantly, the members of this panel, who are entrusted by Congress with looking into the operation of an impact of laws and programs that journalists and private citizens are not in a position to see.

This won't always make you popular with those running the programs or for those who believe that because they are trying to do the right thing under difficult circumstances, they shouldn't be hamstrung by nitpickers who want them to fight under rules that aren't observed by our enemies. One can sympathize with their problem but we can never give in to the temptation to say that whatever means might prove most efficient to achieve an admirable end is automatically justifiable. This nation was not constructed with an idea to providing the most efficient or most powerful government in history, only the freest. Your mission must be to see that those charged with its protection remember that.

Thank you.

Mr. Davis: Thank you, David. Our next panelist is Michael D. Ostrolenk and Michael is the Co-Founder and National Director of the Liberty Coalition, a trans-partisan coalition of groups working to protect civil liberties, privacy and property rights. He has an undergraduate degree in government from the West Virginia Wesleyan College and a Masters Degree in Transpersonal Counseling Psychology from the John F. Kennedy University.

Mr. Michael Ostrolenk: Thank you. My name is Michael Ostrolenk. I'm Co-Founder and National Director of the Liberty Coalition as was just mentioned. We have 61 coalition partners from across political spectrums. My words today are mine alone, though and do not necessarily represent those of our partner organizations.

I'd first like to thank the Privacy and Civil Liberties Oversight Board for inviting me to speak today. The Board was charged with a very important mission. You are ordered to ensure that concerns with respect to privacy and civil liberties are

appropriately considered in the implementation of al laws, regulations and Executive Branch policies related to efforts to protect the nation against terrorism. If I had the ability to change your charter, I'd make it more aligned with the Declaration of Independence, which clearly states that government is instituted in order to protect our inalienable rights to life, liberty and the pursuit of happiness. It does not say that concerns about life, liberty and the pursuit of happiness will be considered as the government goes about its business. Protection, not consideration is what is mandated.

That is what I consider the major problem we in America face today. It is a government which has forgotten what its true purpose is and that its powers, as limited as they ought to be, is only given to it by the consent of the governed.

It has been said repeatedly that 9/11 changed everything but this unspeakable tragedy nor anything else like it should fundamentally change our way of life. When I say "our way of life," I do not mean

our ability to go shopping but fundamental, transcendent principles, which were discovered by human reason to guide us in our political relations. Unfortunately, every crisis we have faced in the United States, including 9/11, has led not to self-reflection and a universal declaration of support for our founding principles, but to an increase in the power of the national security state, a loss of civil liberties, and a great cost to the Public Treasury, to the benefit of politicians, corporations and government agencies.

Although this is not the appropriate forum, in recognition that our foreign policy does have a direct effect on the size and scope of government at home, I would like to suggest that our esteemed leaders consider the wise words of John Quincy Adams, who said, “America is the well-wisher to the freedom and independence of all. She is a champion and vindicator only of her own.”

Now today, we are discussing our collective concerns about the loss or potential loss of our civil liberties during the War on Terror. I want to

clarify two terms before I give time to a few specific issues. One is the term, War on Terror. I would like to encourage everyone to stop using that term. Terrorism is a tactic used by a specific group of people for political purposes and one cannot war against a tactic. War on Terror is a propaganda term used by the State to create confusion and fear in the minds of its citizens. Yes, we were attacked but by a specific group of people. Congress, if they took their oath to the constitution seriously, should have used their constitutional powers under Article 1, Section 8, to declare war. The Declaration of War would have been against a specific foe as opposed to what we now have, which is undeclared, never-ending war against an undefined enemy.

The second term I want to clarify is civil liberties. I use the term to mean all liberties, including economic and social.

All of what I said is important, at least to me, in setting the stage for the issues I want to discuss with the rest of my allotted time.

I will be discussing three issues: the misuse of the material witness statute, medical privacy and the needed protections for national security whistleblowers.

Since the attacks of September 11, 2001, at least 70 men living in the United States have been thrust into a world of indefinite detention, without charges, secret evidence and basic accusations of terrorist links. They have found themselves not at Guantanamo Bay or Abu Ghraib but in America's own federal prison system, victims of the misuse of the federal material witness laws in the United States, for the fight against terrorism.

Congress enacted the current material witness law in 1984, to enable the government, in narrow circumstances, to secure the testimony of witnesses who might otherwise flee to avoid testifying in a criminal proceeding. If a court agrees that an individual has information material to a criminal proceeding and will likely flee if subpoenaed, the witness can be locked up, but in theory, only for as long as is necessary to have him testify or be

deposed.

Since September 11th, however, the U.S. Department of Justice has deliberately used the law for a very different purpose, to secure the indefinite incarceration of those it has wanted to investigate as possible terrorist suspects. It has used the law to throw men into prison without any showing of probable cause that they have committed crimes. Innocent people have become the hapless victims of government zeal because neither the Justice Department nor the courts have honored the letter or spirit of the material witness rules that protects everyone’s right to freedom.

The misuse of the material witness law has been harmful for those who have been wrongly held and is damaging to the Rule of Law. Holding as witnesses, people who are in fact, suspects sets a very disturbing precedent for the future use of this extraordinary government power, to deprive citizens and others of their liberty.

We think the material witness statute should only be used for its intended purposes and

therefore, we recommend the following legislative fixes, which we encourage you all to support.

First, that legislation require the existence of a pending Grand Jury proceeding or criminal trial before such warrants could issue. This would help ensure that witnesses are detailed solely for the purpose intended: to give testimony in a pending case.

Second, the legislation would place time limits on the length of detention, thereby ensuring that individuals would not be held for extended periods of time.

Third, it would require a heightened showing that the detained witness is, in fact, a flight risk. This would protect individuals who would voluntarily respond to a subpoena from being needlessly arrested and incarcerated.

Fourth, it would import due process standards from the Federal Rules of Criminal Procedure, to ensure that material witnesses are informed of the basis of their arrest and their right to counsel.

Fifth, the legislation require that such

witnesses be detained in the least restrictive condition possible, preferably kept from those charged with criminal offenses. This reflects the fact that material witnesses are, as the name implies, witnesses. They are not suspects of any criminal wrongdoing and should be treated accordingly.

And sixth, the legislation require the Justice Department to report annually on the number held under material witness laws and average length of detention. For more information, I would suggest you contact Human Rights Watch and the ACLU.

Another issue that we are concerned with is the loss of medical privacy. The Administration and Congress are pushing for the creation and use of a national electronic medical records web-based data system. The Senate and the House both passed bills this year towards those ends.

The system would place everyone’s medical records on line and available to a wide variety of government agencies, private institutions and companies without the consent of the patient. This

has potentially enormous negative consequences for the sanctity of the doctor patient relationship and the practice of medicine, as well as Americans' constitutional rights. It would seem clear that such a coerce system could and would violate the First, Fourth, Fifth and Tenth Amendments. The Tenth Amendment, because interfering in the practice of medicine and the health care system is not enumerated power under the Constitution.

During the debates over the Patriot Act, I spoke a great deal about how two powers -- Section 215 and Section 505, -- the provision, the National Security letters respectively clearly violate the Fourth Amendment in spirit and in fact and would lead to further erosions, in this case, for medical privacy rights. And this new proposed system of medical records just puts the nail in the coffin of a heretofore universally recognized expectation of privacy concerning our medical treatment records.

I'm sure all law enforcement and intelligence agencies would like to have very easy access to

American's medical records. According to Government Health IT, as reported on August 14th, "The CIA-backed venture capitol firm, INQUTEL, is investing money in a company that sells software used for managing electronic medical records." This is a very disturbing piece of news but not surprising.

However, no matter who wants what, no one should have access to any medical records without the consent of the patient or court order, the latter not being a 215 court order, which in my opinion, is just a rubber stamp.

If we're going to have to live a government coerced web-based system, I would like to encourage you all to make sure the following principles, created by Jim Pyles, an attorney representing the American Psycho-Analytic Association on health privacy matters, are included in such a system and for purposes of brevity, I would just include this in my written comments and I'll give you the principles and there are ten of them.

For more information on medical privacy, I would refer you to the Association of American

Physicians and Surgeons, Patient Privacy Rights Foundation, and the Institute for Health Freedom.

Last but definitely not least, is my concerns for protecting national security whistleblowers. These brave men and women risk everything to come forward within their own agencies or to Congress to blow the whistle on waste, fraud and abuse.

They are our first line of defense in protecting our constitution, our liberties and our money. It is already protected and encouraged, not retaliated against. By retaliating against whistleblowers that report waste, fraud and abuse, which happens most of the time, other employees are dis-incentivized to come forward.

Second, retaliation against whistleblowers is expensive, unproductive, and puts our security, liberties and monies at risk.

Third, whistleblowers who report waste, fraud and abuse are the type of employees that the intelligence and law enforcement agencies need more of, since they are obviously ethical and take their job and obligations to the American people

seriously.

Fourth, retaliation prevents Congress from knowing the facts of potential waste, fraud and abuse and being able to provide good oversight.

We would like to suggest that you consider encouraging the Administration to support any legislation that contains the following general principles:

1. Whistleblowers who report waste, fraud and abuse should be protected against being discharged, demoted, suspended, threatened, harassed, reprimanded, or investigated or having their security clearance revoked.

2. Whistleblowers who are retaliated against should be able to seek relief;

3. In the case of seeking relief, the whistleblowers should be protected against the use of the state’s secret privilege by finding in their favor the privileges asserted;

4. Any person who retaliates against a whistleblower who has reported waste, fraud or abuse, shall be guilty of a felony.

For more information on protecting national security whistleblowers, I would refer you to the National Security Whistleblowers Coalition, the National Whistleblowers Center, the Government Accountability Project, and the Project on Government Oversight.

Those three issues I just addressed are just a few of the many that I am concerned with these days. My colleagues today will be addressing others. I hope you will truly hear our concerns and take them seriously and work with us to make sure our liberties are truly protected. I also hope you keep in mind why the government was created in the first place, which is to secure our rights to life, liberty and the pursuit of happiness and remember, when any form of government becomes destructive of those ends, it is the right of the people to alter or abolish it. Thank you.

Mr. Davis: Thank you very much, Michael and my last panelist is Marc Rotenberg, Executive Director of the Electronic Privacy Information Center. Marc is a graduate of Harvard College and Stamford Law

School and he teaches right here, Information Privacy Law at Georgetown University -- not right here but at Georgetown University Law Center.

Mr. Marc Rotenberg: Thank you very much and I'd like to thank the panel for the opportunity to be with you today. I also wanted to give a special thanks to the Vice Chairman, Mr. Raul and the Executive Director, Mark Robbins, who were both kind enough to meet with the Privacy Coalition earlier this year at EPIC. You survived that and we thank you for spending some time with us.

I was thinking about what I would say to you this afternoon and it struck me that you're in a very difficult position. You've been asked by the President to simultaneously promote the exchange and compilation of personal information across the federal government, to prevent future acts of terrorism and at the same time, to safeguard one of the most precious rights in the United States and that is the right of privacy. I think it would be foolish of me or anyone else to imagine that that is a simple problem to solve.

But at the same time, it also occurred to me that there are people and institutions and law makers that have come before you that have looked at this issue and come with up important answers, legal frameworks that have, in fact, helped safeguard the right of the privacy in the United States.

Now many people in this country have a strong sense of liberty, a strong sense of our Bill of Rights, a strong sense of our Constitution. Not many people are familiar with the federal laws that safeguard the right of privacy. And I'd like to take just a couple of moments to outline for you, two of the key laws that safeguard privacy rights in this country, to suggest to you, what is at issue for this panel as you go about your work.

The Privacy Act of 1974 is perhaps the most comprehensive privacy law in the United States. It creates a structure of oversight and accountability for all federal agencies that collect or use personal information on American citizens or lawful permanent residents. It establishes transparency and oversight -- it even gives people the

extraordinary right to have access to the information about them that is collected by their government. There are legal penalties for the misuse of that information as well as sanctions against federal officers or agency officials who misuse private data collected by the agency.

It is an extraordinarily robust framework for protecting personal information in the information age and even as technology has rapidly transformed, over the last 30 years, I've heard little dispute about the importance of the Privacy Act safeguards to protect the personal information collected by the federal government.

The second statutory framework that I'd like to call your attention to is the Federal Wiretap Act. The Act, which was passed first in 1968 and as the Solicitor General certainly knows, following two important decisions in the '67 term, Katzenburger made clear that the Fourth Amendment would apply to the government interception of electronic communication. But that regime that was established by the Congress in '68 and subsequently amended to

deal with such issues as electronic mail and stored communications, established strong judicial oversight, public reporting, and even the right for individuals to know when they had been the target of a lawful wire intercept conducted in the United States.

These two statutes, these two modern privacy laws, reflect the system of checks and balances in our constitutional form of government. They do not leave to the Executive the authority to decide on its own accord, to what extent an intrusion into private life may be justified. They rely upon the courts to exercise oversight, upon the Congress for hearings and quite significantly, upon an informed public that is routinely notified when systems of records are created within federal agencies, when annual wiretaps are reported by the Attorney General.

It is this system of privacy protection in this country that is under risk today and it is this system of law that if it is not adequately safeguarded, we will see rapidly erode over the next

few years.

Let me give you just a few examples. Now of course, we're familiar with the President's claim that he has the inherent authority to conduct intercept within the United States without judicial oversight and without statutory authority.

I have two points to make about that proposition. One, in making this claim, he has effectively avoided the public reporting requirements that would otherwise be required under a Title 3 wiretap or under a FISA wiretap, which makes it difficult for Congress or anyone else to evaluate the effectiveness of the program, and two, as the President's Civil Liberties and Privacy Oversight Board, I would put to you the question, do you agree with the President's contention? Is it your view that he does have this inherent authority. Your answer to that question determines whether or not the privacy laws that regulate electronic interception within this country, will continue to stand.

Let me give you a second example. You may be

aware in the past week, there has been quite a bit of discussion about a federal rulemaking -- it's extraordinary, by the way, that a federal rulemaking would attract the attention of CNN and the national papers but it has because the Department of Homeland Security has proposed that a system to evaluate cargo entering the United States called the Automated Targeting System, be applied to individuals and upon closer inspection, it turns out that the Department of Homeland Security has been compiling profiles and creating, in effect, terrorist ratings on tens of millions of American citizens. Now if you read this notice in the Federal Register, you will learn that the Department of Homeland Security proposes to share that information with other federal agencies, with local law enforcement, with other government and with private contractors. But it will not give to the individual the right to inspect or correct that information, which the government keeps, about a U.S. citizen.

So my question to you on the second example, is

does the President's Civil Liberties and Privacy Advisory Board agree with the contention of the Department of Homeland Security that under the Federal Privacy Act, it should be allowed to proceed.

I had the opportunity this morning to look at the Privacy Guidelines for the information sharing environment. This is, I understand, one of the key requirements for the Board and I would like, of course, to recognize and thank you for producing these guidelines and I hope there will be some opportunity for discussion but what struck me about the guidelines, when compared with the Federal Privacy Act, was the absence of transparency, the absence of oversight and the inability for individuals to know what information about them is being collected by the federal government and how it will be used.

Well, as I said at the outset, I believe you have an enormous responsibility and no doubt, it is a difficult problem. But if there is one more concern that I can put on the table for you, which

is the same point I made to the 9/11 Commission when I had the opportunity to speak before them, what the United States does in its response to concerns about future acts of terrorism influences democratic governments all around the world, for better and for worse. If we stay committed to an independent judiciary, to the Rule of Law, to transparency, we send a message to other governments that when they face threats, democracy, open government, provides the best solutions, the most robust way to take on the challenges of the 21st Century.

But if we back off these commitments, if we say we can no longer afford judicial oversight or the Rule of Law when the President conducts domestic surveillance or transparency as to the activities of our agencies when they collect data on our own citizens. We send that message as well, to other government and no doubt, we will live with the consequences.

So thank you very much again for the opportunity.

Mr. Davis: Thank you very much, Mark. Madame

Chair, is this the opportunity for --

Ms. Dinkins: Yes, for the members of the Board, if they have questions or comments, please.

Mr. Davis: Well, since I was the introducer, let me ask the first question. I would like to ask Caroline and David and Mark, I think, summarized what I was really getting at in his very eloquent statement.

From the ACLU to the American Conservative Union, which ordinarily one would assume spans a certain etiological spectrum, I heard one very clear message but one unclear message. The clear message from Caroline on the NSA Surveillance Program is that the United States should not conduct such a program, “without clear legal authority to do so and at the cost of Americans’ privacy.” And from David’s comments, a very similar comment -- “I’d like to emphasize our view that we have never believed that the issue is whether the government can or should under certain circumstances, conduct such surveillance but that such activities must be conducted in compliance with our constitution and

existing law." So you both seem to agree that there should be a basis in law for such a program and there is debate whether the President can act unilaterally under the constitution or under the rationale that the President's Attorney General used versus Congressional authority. So my question to both of you and perhaps to you, too, Mark, is would you support Congress, whether or not the President is correct that he had the constitutional or legal authority to undertake this surveillance program, would you support Congress amending, if necessary, FISA in order to permit this program, if you were convinced that the Fourth Amendment, which does and has been interpreted to mean reasonable searches, that Congress as a body representing all of us, could undertake without compromising our national security efforts to intercept these terrorists, that Congress should amend FISA or the wiretap law or some other law and would you support their attempting to do that consistent with your view of privacy and civil liberties rights?

Ms. Fredrickson: I'll just answer that briefly

but I'd first say that actually, as a nonpartisan organization based on principles, we work quite a bit with the American Conservative Union when --

Mr. Keene: You keep it a secret!

Ms. Fredrickson: We keep it a secret? But it's true, there are a lot of places and with the groups that are represented up here as well, because our focus is on the issue and how to be effective. But I would say that I think it is very premature to start questioning whether we should support Congress amending FISA until we actually have a much better understanding of what the program is.

I think when members of Congress, by and large, don't have a very great grasp of what the program is, how many people have been under surveillance, what's been done with the information, how is it being protected, how is it being used? I think until that investigation and oversight happens, I think we couldn't possibly begin to answer whether FISA should be amended.

Mr. Keene: As the Board will recall, shortly after the NSA program became public, the Senate

Judiciary Committee did, in fact, hold hearings and the Chairman of the Committee, Senator Specter of Pennsylvania, suggested to the Administration that he believed that as the program was being run, it was not in compliance with the law and he said if the law is inadequate, tell us how it is inadequate to that the Congress can consider whether it should be amended to allow this kind of activity and the Administration demurred on saying they didn't think there was any necessity and ultimately fell back on the Inherent Powers Doctrine.

There are two questions. One is the question of is it necessary, should you do it? And the second question, which is just as important in a nation that lives under a constitution and the Rule of Law is if it is necessary and if you must do it, how do you do it? And if it is, in fact, necessary then it is our view that the Administration ought to go to the Congress and ought to get the law amended. The Inherent Powers Doctrine clearly exists under certain circumstances but Presidents in the past who have attempted to utilize it, Harry Truman and the

steel seizure case back during the Korean War have found out that it isn't as expansive as they thought it was and even -- I would be reluctant to suggest to any president that that is something that he should rely on because if he does, somebody will and you're on a slippery slope with an undefined power. If something can be done efficiently with Congressional approval and you can meet your objectives, it seems to me that that's the way it ought to be done and we would support the Administration going to Congress, dealing with the Congress, making the case for what is needed and the Congress, if it's reasonable, giving him the power necessary.

Ms. Dinkins: Questions of any other members of the Board?

Mr. Raul: Thanks, Carol and as Lanny indicated, thanks for all of those, I think, very thoughtful and very helpful presentations. In particular, I think you are raising with us the problems with the material witness statute that you've identified, is very important I believe this

may be the first occasion that's it's been addressed directly with the Board. So I appreciate both -- Fredrickson and I think, Mr. Ostrolenk, maybe others, raising that.

Watch list issues -- we've also discussed -- maybe I'll throw out a couple of questions for follow up in the interest of time. If you have any information quantifying or compiling information on issues, problems with watch lists that you're in a position to bring to our attention, I think that would be very helpful. I'm aware of various studies and reports from within the government. If you have any outside information that can be shared with us, we'd certainly appreciate that.

If you have suggestions on approaches to future public interaction for the Board, future meetings -- this format or other formats, we'd be interested in hearing that. That may not be something that you are in a position to address right now but if you have ideas for that, we'd certainly welcome it. We certainly would like to maintain the dialogue.

On the notion of transparency of information

collected and retained by the government was mentioned by Marc Rotenberg and others. Obviously, it's at least a challenge in an area involving the need for secrecy and with classified information and so on, it's a challenge to provide a degree of transparency and reconcile that with what many believe is appropriate secrecy. If you have any suggestions on those can be reconciled in way that would give some reassurance to the transparency interests that you've mentioned but would also preserve what many believe are legitimate needs for secrecy and that information -- we'd certainly be interested in hearing that as well. Thank you.

If you would like to respond now or otherwise, I'd certainly be willing to receive that information whenever you have it to share with us. Thank you.

Ms. Dinkins: Questions from the Board? Would the officers care to pose any questions or make any comments?

Mr. Alexander Joel: If I could just make one or two really quick comments. One is, Marc I know you just got the privacy guidelines this morning and

haven't a chance to study them but if you go back and look, you'll see the guidelines certainly require agencies to continue to comply with existing statutes. We have other explanatory materials up on www.ise.gov that provides some FAQ's on that so we would expect agencies to certainly continue to comply with the Privacy Act very important. We're going to issue additional guidance and we have a committee structure set up to try to surface those kinds of issues that are going to happen across the agencies, consult closely with the Privacy and Civil Liberties Oversight Board with the Privacy Act, a very important foundation for privacy and we'll continue to be -- I just wanted to make that quick point.

The other is -- you know, Caroline, we certainly agree with you that we have to be both safe and free and it's a balancing -- I don't know if you like that metaphor but it's one that I find helpful and this is part of the discussion of how do we achieve the right balance. In my mind, when you have scale people think of, when you do more on the

national security side of things, you'd necessarily lose out on the privacy and civil liberties side. Other people think if you're doing more on the privacy and civil liberties side, you lose out on the national security side. Our challenge is to do both. How do we do both? Sometimes it's by not doing as much on one side. Sometimes it's by adding more to the privacy and civil liberties side and I view our office as performing that role within the Executive Branch. You're performing your role outside. The government -- the courts and Congress obviously have very important roles to play as well but our role within the Executive Branch is trying to advise our folks so that we can add safeguards as we try to do new and different things on the national security side. But I'd welcome this dialogue and like for it to continue. So thank you for having us.

Ms. Fredrickson: Just a brief comment in response. I agree with you that we don't think there should be a balancing in the sense of trade-offs between civil liberties and security. We don't

think that's necessary and it's certainly not consistent with our view of our constitution and what really makes America such a wonderful country and a beacon for the rest of the world in terms of our democracy and our basic rights that we have here in the United States. I think we very much support the role of the privacy officers. We're very supportive of the legislation. We just think you need more authority, similar to the Board. You need to actually be able to have subpoena power and you need to be able to do some real oversight and we will support trying to give you that power.

Mr. Keene: We agree with that, that it's not a trade-off. The obligation is to provide for the defense of the American people and the American continent, the American nation without sacrificing the reasons for which we all love it. And it's -- you don't make that trade-off. You do consistent with your traditions, not saying, well we'll do this today and something else tomorrow.

Mr. Rotenberg: You might forgive me if I'm a little impatient on this point. But you see, that

analysis, that conclusion was reached a long time ago. I mean, it's inherent in the U.S. form of government, of checks and balances and requirements of openness and the question really today is whether it's going to be effectively applied, right? I mean, we have established here an oversight mechanism within the Executive Branch of government. But if you study the structure of privacy oversight, both in the U.S. and in other countries, the first thing that you recognize is that to be effective, the agency has to be independent because even well-intended people seeking to protect privacy will necessarily be under institutional pressure to move in the direction, the desire the institution wishes to go. This is no surprise. So -- I mean, of course, Alex, we should be able to achieve both security and civil liberties. There's never been any dispute about that. But the real question is whether this means an oversight can be made to work and I think the problem, perhaps, is more serious than people realize. Because the guidelines, as compared with the Privacy Act, do not provide

American citizens the rights that are otherwise established in law, that were enacted by the U.S. Congress. So what do we say at this point? That we can no longer afford to give people those rights?

Mr. Ostrolenk: Actually, I would just like to follow up on Mark and ask the Board if you all will be responding to Mark's two questions he asked earlier. One, I believe, was on the President's inherent power to do the NSA, domestic spying and I don't recall what the second one was but will you be responding to him today and if not, will you respond at a later date?

Mr. Davis: Well, I would like to respond because I was quoted in a couple of newspapers saying that I was impressed with the lengths to which the individuals involved in the surveillance program went to be sensitive to civil liberties and privacy rights, which I was looking for and which I found and was positively impressed. But that doesn't mean that I think that the President has the right to decide without going to Congress. I'm open to the debate and I've read the legal arguments but

I would prefer, in a system of checks and balances, that we not have a -- what is sometimes described as a unitary Presidency but that we go back to the conservative tradition of checks and balances and that is the reason that I asked the panel and Caroline and David whether -- if I'm right that this program is important and necessary and if the President is right that it is, wouldn't it be better to go to the Congress, do the oversight and find a solution that lets us keep the program and even if there is good debate between good scholars as to what Presidential inherent authority is or is not, why not, for the purposes of the American people, allow their Congress that they freely elect to be part of the process of developing the program. So for me, the answer is, I'd prefer that if it were possible, without compromising the security and the purposes of the program.

Ms. Dinkins: Thank you. And we thank the members of the panel. We very much appreciate your hard work to prepare and your time to be here and bring your thoughts and your ideas to us. We will,

I'm sure, be talking with you further.

As we transition from one panel to the other this afternoon, we will take a few minutes to have time for questions from the audience and we would ask that you limit yourself to 60 seconds so that we can have an opportunity to be sure that we hear from all of the invited panelists. And we have standing at the microphone, John Coghlan, our Staff Assistant and for those who may have questions of the Board but not the opportunity to ask them today, we invite you to send your thoughts or your questions to us at our web page, which is www.privacyboard.gov. Sir? Please. If you would state your name?

Audience Member #1: Hundane from [inaudible] with the United States Bill of Rights Foundation and my question is to the Board and perhaps maybe Mr. Davis might want to answer it. I'm not sure, being that he has referenced his statements in the papers. I was wondering, could you compare the so-called -- like the Gang of Eight, I think they were called, who were briefed on the NSA wiretapping program and they were given a special briefing. I was wondering

if you have a position, just sort of describe the difference between what you have seen and what reports have been made to you in comparison to the Gang of Eight and as a tag-on to that, do you see a change in your role when the new Congress comes into power? Do you see it changing your role here but more specifically, what is the difference between what you've been exposed to on the NSA wiretapping versus what Congress has been exposed to?

Mr. Davis: I'll defer to my colleague, the Chair, if I'm incorrect but it's my understanding that we were read into the program with the functional equivalent of information of anybody else who was read into the program including the members of Congress.

Ms. Dinkins: Thank you. And that certainly was my understanding. We have offered to and are willing and eager to meet with members of Congress who have an interest in the work of the Board and we look forward to having that opportunity when invited. Yes, please?

Ms. Graves: Hi Ms. Dinkins, it's Lisa Graves.

I'm the Deputy Director for the Center for National Security Studies and I had a question or a couple questions that are very brief, about the Foreign Intelligence Surveillance Act violations by the NSA and this Board's role and they are both related questions.

The first is whether this Board intends to take positions on legislation or whether it is going to ask to take a position on the legislation that was circulated and endorsed by the White House earlier this year, on the so-called Terrorist Surveillance Program and it's authorization to conduct this program without the judicial oversight, the individualized judicial oversight required by statute in the constitution but that actually goes to a related question, which is whether this Board has been informed about the number of Americans whose conversations have been wiretapped over time, whether you've been informed about how any Americans were wiretapped in 2001, 2002 to the present, each year. How many Americans -- data, phone data, financial data, has been obtained by the NSA? Do

you know the answers to those questions? Were you briefed with that specificity on those numbers and would you make those numbers public?

Mr. Raul: I'll try my hand at those. They are probing and difficult questions. With regard to positions on legislation, the statute does give us a mandate to provide advice and oversight with regard to development and implementation but the development of laws, policies and other actions. So I think it is appropriate for the Board to provide its views on the development of legislation and on particular draft legislation but I would submit that it's appropriate for the Board to do that in the context of the Executive Branch location where we were placed by the Act of Congress. So I believe that would be more properly viewed as internal advice.

We did receive briefings and had an opportunity to engage certain members of the Board based on the timing of when certain drafts of the legislation were being considered. We were provided some briefings. Really, I think, at the invitation of

the Attorney General on some of that legislation.

With regard to the question that you asked on the data, that obviously is a very sensitive matter, a core element, I think, of the classified program. I think all it would be appropriate to say is that we did receive a detailed briefing with information of the kind that you described and I think that our involvement with that program will likely continue.

Ms. Graves: Briefly, has the Board or have Board members recommended that information be made public on the same basis that Congress currently requires -- numbers, just the raw numbers of foreign intelligence, wiretaps that are authorized by judicial officers be made public. Have you urged that that information be made public and has that been rejected?

Mr. Raul: With respect, I think it is important for us to maintain the confidentiality of some of the recommendations that we might or might not have taken. So I can't address really the substance of the question but only to note that part of our ability to provide advice within the

Executive Branch of the President and agency heads really is the ability to provide advice confidentially as well as of a public nature, which we're doing in this forum and in our report and so on. But to share some of the private views that we might have, I think would undermine our ability to be effective as the statute contemplated or at least potentially could be.

Ms. Graves: So is the Board no longer going to be making their private views public? Then I'll quit, I promise. But I'm curious because it seems to be inconsistent in some ways.

Ms. Dinkins: Lisa, I think he has answered your question. Thank you, though. Sure.

Mr. Davis: But I would like to add my own personal view that doesn't necessarily reflect my colleagues. Congress put us in the Office of the President. We didn't put ourselves in the Office of the President. Had Congress wanted us to be an independent agency, they would have created us as an independent agency. So if you hear today, responses from those of us that are somewhat ambiguous, in

direct answer to the question you asked our Vice Chair, Allan Raul, I would read the Act and ask yourself why Congress did what it did, rather than asking us whether we're supposed to be both an independent oversight authority and within the Office of the President and if so, how do we do that? That's an open question that none of us up here have been able to quite figure out.

Ms. Dinkins: Thank you. Yes, if you would please, we are going to move to our next panel and then we will have another opportunity between this panel and the third panel for additional questions.

Mr. Ettington: If I could just briefly -- 20 seconds -- 20 seconds.

Ms. Dinkins: Twenty seconds.

Mr. Ettington: I'm Patrick Ettington, Senior Policy Advisor of Representative Rush Holt of the House Intelligence Committee. I appreciate your commitment, Ms. Chairman, to testify before the Committee and I will carry that message back to Mr. Holt this afternoon. Thank you.

Ms. Dinkins: I will now call on our member,

Ted Olson, to introduce the second panel, please.

Mr. Olson: I will do this briefly, if you'll forgive me because we want to hear from you rather than us. I will say only this in preliminary statements that we feel -- or at least I do -- strongly that security and civil liberties are not opposites. Security is a civil liberty. The right to walk freely in this country without being blown up is a civil liberty and so there are all of those things that we have to be mindful of. This program today is an exceedingly important part of our mission, to hear these points of view. We have a great deal to learn in order to perform our statutory responsibility and this is today, neither the beginning nor the end, by any means, of that process, of our efforts to hear what we need to hear and learn what we need to learn in order to do our job and we have been -- it is not correct as one of the witnesses said, that most of our meetings have been on the telephone and things like that. Virtually all or all of our meetings have been in person involving all of us. We have personally

visited, in some cases, more than once, the National Security Council, the FBI, the Department of Justice, the National Security Agency, the White House, the National Counter-Terrorism Center, the Treasury Department, the Terrorism Screening Center, members of Congress. We visited with the National Security Advisor, the White House Counsel, the Director of National Intelligence, the Director of Central Intelligence, the Chief of Staff to the President, the Attorney General, the Deputy Attorney General, the Director of the FBI, the Director of NSA, the Markle Foundation, top U.S. government privacy officials, numerous other officials in the United States government. We have been cleared to review and have reviewed numerous highly sensitive classified programs. We have had access to anyone that we have wanted to have access to, to date. We have been able to ask any questions that we've wanted to ask to date and they have been answered. We are in a process of doing everything we can to learn from those officials in the government and persons outside the government that have issues of

concern to us. So, we want to do this job conscientiously and we're going to continue.

Now, to help us, this second panel, first of all, I will introduce you both. Brian Walsh is a Senior Legal Research Fellow in the Heritage Foundation Center for Legal and Judicial Studies here in Washington. He directs that foundation's projects in countering the abuse of the criminal process, particularly at the federal level and has a mandate, all in various different areas like that. He has also worked with the Homeland Security Department and before that, practiced commercial litigation with a very distinguished law firm in Washington.

Mr. Dempsey is a member of the Markle Task Force on National Security, an organization that has been -- it involves senior executives from the information technology industry, public interest advocates, experienced policy makers, experts in privacy, intelligence and national security. He has produced three extremely thorough and valuable reports in this area. Jim has also served as a

Policy Director at the Center for Democracy and Technology and I could go on and on.

Both of these individuals have a wealth of experience and understanding in this field. So we're very, very grateful that you'd be here with us today. Brian?

Mr. Walsh: Well, thank you very much, Ted and thank you also, Chairman Dinkins and the other members of the Board, officers. It really is a privilege to address you today and to discuss these hugely important topics that are a matter of current public debate and on the forefront of everyone's mind. So I just want to offer a few thoughts today on how to foster a productive civil and informative debate on privacy issues, especially in the context of prosecuting the War on Terror.

Before I do so, I'd just like to mention that all of these opinions today are my own and do not reflect -- necessarily reflect the opinions of the Heritage Foundation.

But I've got really just three brief goals that I want to address. The first is to provide an

analytic framework for analyzing and discussing risks to real and alleged privacy interests. The second is to set forth the general principles for safeguarding civil liberties when using information technology to combat terrorism and the third is to apply that analytic framework and those principles in a very general manner and just to touch on the use of data mining as an example, that technology, to detect and prevent terrorism.

I'm going to delve slightly deeper into data mining in a few minutes but I'll provide a working definition for those who might be wondering now what my definition is and that is, it's using systems that combine technology for acquiring and sharing disparate data with tools for analyzing it in order to identify relationships among that data that are potentially significant. And I say potentially, of course, because not all of the hits will be ones that are real. Sometimes you have false positives.

I'm specifically considering data mining used to detect and prevent terrorist activity but there are other relevant applications of data mining. The

business community has, for years, been using what we now call data mining and they've used it for fraud protection and detection, among other things and to some extent, all Americans should be happy about that piece because it lowers the interest rate on our consumer credit.

They also use it to quickly identify identity theft and most of the experience and innovations with data mining technology probably are in the private sector and the government probably has quite a bit to learn from the private sector about data mining technology.

But there is a problem in the way that we -- setting aside data mining for a moment, there is a problem in the way that we debate privacy issues and I'd like to just state that problem. The public debate often does not rise to the level of discourse that is necessary so that the -- to enable the average American to draw informed conclusions.

In addition, this inadequate issue development hinders policy makers and I think in some instances, it's to some people's interests to make that happen

because it does get confusing and blurs some of the distinctions that I think are important.

Some national security advocates speak as though they accept without question, almost any method of data acquisition and analysis, if it seems to have a reasonable shot at finding some terrorist activity. Some privacy advocates frame almost any identifiable privacy interest in absolute terms. In their view, government may never violate what they deem to be private. But just because an individual wants to keep something private doesn't mean that he or she has a legally cognizable interest in keeping it private.

I think that's an underlying problem in the public debate. Some seem to thrive on blurring the distinction, on both sides of the debate, between policy preferences and choices on the one hand and legal and constitutional analysis on the other. And much of the debate proceeds with no acknowledgement of that crucial distinction.

Just speaking about policy preferences as though they were constitutional mandates, our

fundamental principles of law of nature is both sloppy and manipulative. The result is public confusion and disconnect in the midst of this crucial discussion.

In order to address that, I would just like to discuss or set out some ideas for an analytic framework and I'll start with the premise that technology is neither inherently good or inherently evil. Technology is a tool. Radiation technology is one example. It may be used as a weapon or as a cancer treatment and as mentioned, the private sector has already demonstrated that data mining -- the same information technology that can be misused to infringe real rights and facilitate government abuses, can be developed into a tool to detect credit fraud and identity theft. I think there is a real reason to believe that data mining could be used for similar good purposes in detecting terrorist activity.

The best analysis of this has been mentioned multiple times, which is that privacy interests, civil liberties on the one hand and national

security are not a zero sum game. There are a lot of innovations still to be done in technology and technology -- this type of technology, in particular, is still in its infancy. So we can expect, I think, that there will continue to be advances but we need some guidance in order to make sure that the advances come with appropriate safeguards. But before we do that, we really want to think about what the right framework is for analyzing these issues.

Americans have always -- of course, must always be diligent to protect against unwarranted government intrusions into their personal and private affairs. It was Jefferson who said that the natural progress of things is for liberty to yield and government to gain ground and I don't know any Americans who are willing to jettison their fundamental rights in order to prosecute the War on Terror.

So the first step is to analyze the constitutionality of any new or existing technology. In the text of the Constitution itself, is of course

a starting point.

Now the Constitution never mentions the word privacy. It primarily boils down, in most instances, to a Fourth Amendment analysis and the touchstone of the Fourth Amendment analysis, of course, is reasonableness, an inherently flexible standard. The flexibility of this reasonableness standard implies that there are few absolute or bright line rules defining what is an unconstitutional invasion of privacy and what is not.

Not the only reason but one of the reasons why Fourth Amendment jurisprudence is -- this is not the only reason but one of the reasons why Fourth Amendment jurisprudence is populated with rules and counter rules, exceptions and counter-exceptions. Of course, it shaped the law to reflect what is reasonable under the circumstances.

Our analysis of what is reasonable is heavily affected by the nature of the threat. In Kilo against the United States, a 2001 opinion by the court, authored by Justice Scalia, the court

determined that the use of sense-enhancing technology -- in this case, heat detection technology, to gather any information regarding the interior of a home that could not otherwise have been obtained without physical intrusion in the constitutionally protected area of the home, constituted a search. Because it had been executed without a warrant, it was presumptively invalid, presumptively unconstitutional. That was probably the right result but this is an admittedly contrived example but let me offer it because I think it's instructive.

Suppose that a suitcase sized radiological weapon was detonated in Cincinnati and we learn after the fact that the weapon was made in someone's home. It's easy to do so and that several of the terrorist comrades are still at large. If we had the technology to detect the amount of radioactive materials sufficient to make a weapon from outside a home, might we conclude that it would then be reasonable to do so?

Again, in sum, the nature and extent of the

threat we face determines the reasonableness of the intrusion on America's privacy.

Nevertheless, fundamental constitutional rights, including the right to be free from unreasonable searches and seizures, must be protected in all new government applications of information technology.

Next, we should also demand that all three branches of government respect and abide by the separation of powers. Along with federalism and the text of the constitution itself, the separation of powers is one of our ultimate checks and balances against government overreaching. It's often tempting to attempt to rein in the power of one branch or expand the power of another in order to achieve a desirable short-term policy goal. But the long term cost of succumbing to that temptation is a loss to Americans' understanding of and respect for the constitutional and prudential bounds of all three branches. Giving into that temptation also undermines each branch's understanding of and respect for the other two branches.

Now, Congress has considerable power to decide certain important questions of constitutional magnitude and of policy during wartime. For example, Congress has express power to punish violations of the laws of nations. Congress has express power to establish uniform rules for military tribunals. Once Congress has properly exercised the power to fashion tribunals for enemy combatants, its prescriptions are essentially final. It's been given an express constitutional mandate.

Yet Article I of the Constitution does not vest in Congress some sort of unlimited authority to define the Executive Branch's power and that power is granted or even implied to the Executive Branch in Article II. Nothing in Article I grants Congress authority over military intelligence decisions.

Again, neither the Executive Branch nor the legislation branch is supreme over the other and part of what we're seeing, I think, in the interplay on the Terrorist Surveillance Program is the normal constitutional function, which is that the two branches jockey and position to try to protect what

they are supposed to be able to protect. It's their self-interest, it protects the encroachment from the other branch.

As to the programs like the Terrorist Surveillance Program, the operational intelligence for military activities has always been within the sole province of the Executive Branch. Congress can oversee it. Congress can de-fund it. But it does not have operational control.

The next part of the analytic framework is the legal framework, beyond the constitutional framework and in that discussion, all relevant laws should be considered. I have a concern about that, partly on -- there is one prominent recent example in which this did not happen and that was the debate over the NSA's so-called Call Detail Collection Program, which is a data mining style program. One publication's front page headline on May 11, 2006 said that the NSA was collecting billions of call detail records for use in detecting and monitoring terrorists and their calling patterns. Now I've read scores of articles and listened to or watched a

similar number of news reports asserting that this program violates the Electronic Communications Privacy Act, specifically Sections 2702 and 2703 of Title 18 of the U.S. Code. But Section 2709 of Title 18 specifically authorizes the FBI Director or his designee to collect such information for national security investigations. Section 2709 further authorizes the FBI to share this information with any other federal department or agency, presumably including the NSA. The only reference to Section 2709 that I've seen in the mainstream news was by a single commentator who discussed it in passing.

Now I'm not saying or asserting that the FBI was involved in the NSA's Call Detail Program or whether the program was called out in accordance with the provisions of Section 2709. But Section 2709 should have been part of the public debate in mainstream new sources and eventually, of course, the news sources came back and admitted that some of their initial allegations about the illegality under the Electronic Communications Privacy Act had not

been well founded.

Finally, after the constitutionality and legality of a program have been determined, what are left are policy choices. Now policy choices are important and they should be debated honestly. But they are not constitutional; they are not legal choices, they are policy choices. They shouldn't be clothed in language suggesting that they are compelled or prohibited by the constitution or existing law. I wonder whether much of the confusion and disconnect among Americans on the constitutionality, legality and achievability or desirability of current methods of conducting the War on Terror are really based on unidentified and unstated differences and assumptions about the nature of the threat and whether we are really in a shooting war, which I believe we are.

Finally, we must always, in all circumstances, protect these constitutional liberties but from a practical perspective, there are two distinct types that we need to look at.

One is that we should never countenance,

intentional or systemic, constitutional violations. That is, we shouldn't design a data mining system in such a manner that if it is properly used, it would violate fundamental constitutional rights. That goes without saying.

Second, we have to realize that government can always violate some rights. It always has that power because it has power. And even an information system that is properly designed, using state-of-the-art technology still poses the potential for misuse and abuse. Our goal in this second instance must be to be diligent to prevent, identify and punish such violations.

Impositions on meaningful privacy interests must be justified. They must be justified by the nature of the threat. For instance, any increased imposition on American privacy interests must be justified by understanding the significance and the severity of the threat being addressed; the less significant the threat, the less justified the intrusion is, as I mentioned.

The effectiveness of the method should be taken

into consideration. A less effective method should not -- we should not allow a more significant privacy intrusion. And we need to understand and limit the intrusion on privacy. Not all intrusions are justified simply because they are effective. As an example, not necessarily the best but strip searches at airports would prevent people from boarding planes with weapons but the cost would be far too high.

Finally, we need to look whether there is less intrusive means, regardless of how justified the intrusion may be, if there are less intrusive means of achieving the same end at a reasonably comparable cost, the less intrusive means ought to be preferred. There is no reason to erode American's privacy when equivalent results can be achieved without doing so.

We should keep in mind as a final thought that any system developed and implemented must be designed to be tolerable in the long term. The War on Terrorism, like the Cold War before it, is one with no immediately foreseeable end. Thus,

excessive intrusions may not be justified. Again, it goes back to the reasonableness analysis, because the lapse of -- termination of hostilities may be far in the future and policy makers must be restrained in their actions in the short term because Americans might have to live with their consequences for a long time. Thank you.

Mr. Dempsey: Ted, thank you for that introduction. Madame Chair, members of the Board, colleagues, good afternoon. Thank you for the opportunity to participate in this public panel. As Mr. Olson said, I am Policy Director of the Center for Democracy and Technology but I am here today to speak on behalf of the Markle Task Force on National Security in the Information Age.

I submitted, through the staff, a statement for the record, which I will not read now but instead, address some key issues and then look forward to responding to your questions.

First of all, congratulations on holding this public meeting. It is part of a broader, very important process of dialogue as our nation strives

for answers to some of the challenging questions posed by the War on Terrorism.

The Markle Task Force, in its third report, stated, “we urge our government to engage in a public debate, to the extent possible while maintaining national security, about the guidelines and rules that govern information sharing. This debate should also seek to clarify agency missions and address the requisite civil liberties and privacy protections.” This debate, of course, will occur and should occur in multiple forums, this board being one of them.

I will focus my comments today as the Markle Task Force has done in its work, on the question of information sharing. Earlier this year, the task force issued its third and final report, urging a sense of renewed commitment to the establishment of the information sharing environment. And in recent weeks, two important steps have been taken in the development of the information sharing environment, which the task force has recommended and which was mandated by the Intelligence Reform and Terrorism

Prevention Act of 2004, namely the issuance last month of the Information Sharing Environment Implementation Plan and secondly, the issuance just yesterday of initial Privacy Guidelines for the ISE.

Primarily, I'm going to talk about and give some reactions to the guidelines. It's important at the outset to recognize what the ISE Privacy Guidelines do not address. First of all, they do not address collection standards. In particular, they do not address the predicate that should be necessary and the process for the initial collection of information. The Markle Task Force did not address this question in-depth either, although the task force did stress that there had to be a predicate for any collection of personally identifiable information.

The guidelines also do not address the question of agency roles and missions. The Markle Task Force approach was based in part on a clarity and a clarification of authorized uses, which in turn requires careful consideration and definition of the appropriate roles and missions of agencies and

offices. That is addressed, the question of roles and responsibilities is addressed neither in the Information Sharing and Implementation Plan nor in the Privacy Guidelines.

Until those questions are publicly addressed -- that is, which agencies have which missions, who is responsible for the collection of intelligence information, particularly inside the United States, particularly against U.S. persons, what is the role of the military in domestic intelligence? What does domestic intelligence mean? Until those questions can be answered, they will be left to the assertions of individual agencies with the risk not only of civil liberties intrusions but also duplication of effort and the expenditure of resources on non-productive forms of information gathering and analysis.

Also it is important to recognize the limitations of what was issued yesterday. The guidelines are appropriately described as a framework. They focus more on process than on substance. To take just one relatively small

example, the guidelines issued yesterday state that agencies shall, “Take appropriate steps when merging information about an individual from two or more sources to ensure that the information is about the same individual.”

Now first of all, we all expect that the agencies are taking steps to ensure that already. But the guidelines do not say what appropriate steps are. So the guidelines tell the TSA, for example, to be careful when matching Ted Kennedy on the Terrorist Watch List with Ted Kennedy on the flight to Massachusetts. But they did not begin to tell the agencies, TSA or any other agency, how to actually go about doing that.

To take another example, the guidelines appropriately say that each agency shall implement adequate review and audit mechanisms, to ensure compliance with the guidelines. But they do not have any specificity as to what is an adequate audit, what one should be auditing for, who should be audited, who should have access to the audits. The task force, in its third report on pages 67

through 70, gave some concrete recommendations, not that the task force report is the sole repository of knowledge on this point but the task force did put forth some specificity as to how auditing should be conducted, not only at the agency level but at the individual level and what are some of the technologies for carrying out auditing.

A third example, the guidelines call for redress mechanisms to be put in place to address complaints from persons regarding protected information about them that is under an agency's control. Again, the guidelines offer no further details on how to go about setting up a redress mechanism and particularly, they don't address the threshold question, which is that a number of agencies won't even tell you whether they have information about you or not, in the first place. So how can you exercise a redress right if you don't know what information exists and what it says. The example was cited by the prior panel about the risk assessments being performed by the Department of Homeland Security through Customs and Border

Protection Bureau against travelers, including citizens entering and leaving the country and there is no process. In fact, the proposed Privacy Act Notice for those risk assessments specifically purport to exempt the risk assessments from the Privacy Act disclosure rules and that those disclosure rules are the hinge for the redress rules.

I could cite other examples in the guidelines. Of course, there will be circumstances in which you don't want to tell a person what you have about them. But then you've got to have some alternative redress mechanism.

So at the end of it, the guidelines have little to say about what agencies should be doing differently than they are doing now. So therefore, we have to look at the guidelines as the beginning of a process and the challenge, really, is to put some meat on these bones. I almost see a process leading to a set of appendices or attachments to the guidelines, to take each one of these issues: data accuracy, entity resolution, or watch list fidelity,

auditing and has individual, more detailed appendices to those guidelines.

In its third report, the task force, Markle Task Force, stressed that guidelines such as these will have to be developed incrementally. Specifically, the task force said, “In an area this complex and dynamic and so affected by evolving threats and rapidly changing technologies, the guidelines should be revisited at regular intervals to determine what is working, what is not, what needs to be changed or improved. There inevitably will be ambiguities or unanswered questions. These should be addressed explicitly, not ignored or exploited to avoid the laws’ requirements. We, the Task Force, recommend an annual or biannual review of guidelines by the DNI or other senior Executive Branch official charged with overseeing their implementation.”

Speaking for CDT, I look forward to contributing to that process and I know that other members of the Markle Task Force also remain committed to working to resolve the hard issues.

Representatives of the Office of the Privacy Officer at the DNI have already called me to say that they look forward, that they are wanting to convene such a meeting and I think really should be seen as a series of meetings and a process to put some meat on these bones.

I would like to address another aspect of the task force's third report and that is our recommendation on U.S. persons data, which is one of the hardest issues facing information sharing initiatives. The task force recommended the development of an authorized use standard for sharing and accessing information lawfully collected by or available to the U.S. Government. Again, we didn't address the question of collection standards but once the government has it, how can it be shared, when it relates to U.S. persons?

We did not recommend abandonment of the concept that U.S. persons are entitled to special protection nor do the guidelines that were issued yesterday. The guidelines issued yesterday were premised upon the principle that U.S. person data is especially

protected and treated.

We did not recommend lowering standards on collection of U.S. person data and we did not recommend the expansion of agency missions to permit targeting of U.S. persons, for example, by agencies traditionally focused overseas.

What the Task Force said is that authorized uses are mission or threat-based permissions to access or share information for a particular purpose that the government, through an appropriate process, has determined beforehand, is lawfully permissible for a particular employee or a particular unit or a particular component, a particular agency.

In this regard, I have another specific comment, I guess, or criticism of the guidelines in that they talk about purpose specification but they say that each agency shall adopt internal policies and procedures requiring it to ensure that the agencies' access to and protected use of information available through the ISE is consistent with the authorized purpose of the ISE. But the ISE is a broad -- has a broad purpose of promoting the

sharing of information relevant to terrorism.

What the rules should really say is to ensure that the receipt of information or the sharing of information is consistent with the authorized purpose and mission of the receiving agency or the requesting agency. So in the Markle Task Force report, we cite some examples of how this would work in terms of the CIA. The CIA is primarily prohibited from being operational inside the United States. If some U.S. person data is relevant to some overseas activity of the CIA or perhaps tracing of financing, terrorist financing overseas, then it would be appropriate perhaps, to share U.S. person related data with the CIA, not for the purpose of the CIA operating domestically but for the CIA to use in its mission to investigate terrorist financing overseas. And we give other examples.

This is one way in which I think the guidelines, in this process -- I mean, they are a day old but they were issued, I think, with the understanding that they would be re-examined and improved, now that they are out there in the public

light. We had urged, really, that they be truly open for comment before being issued. I understand to some extent, that the sort of Executive Branch issues at stake there -- okay, now we've got them. Now let's all engage with them and take them to the next level.

In addition to a clear designation of appropriate roles and missions of agencies and offices, the Markle approach requires careful monitoring and oversight of the actual uses of information and I want to highlight what I think is one potentially very important element of the guidelines issued yesterday, Section 4, on page 3. It requires each agency to identify its data holdings that contain U.S. person data that might be shared through the ISE and to identify specifically the rules within the agency that govern the use and sharing of that information. This catalogue of information, I think, will be very helpful, not only to the agency privacy officers, not only to this board, not only to the program manager but to the agencies themselves, to get a sense of what they

their counterpart agencies hold, to the DNI and to Congress.

So obviously, there is a need for ongoing oversight by this board and others and for much greater detail than we see in the guidelines issued yesterday. We welcome them as an important step but only as an initial step and with that, Madame Chair and Members of the Board, I look forward to your questions.

Ms. Dinkins: Thank you, Mr. Dempsey, Mr. Walsh. Question from the Board? From the Privacy Officers?

Mr. Joel: I think Jane and I would like to respond to some of the comments from Jim on the privacy guidelines if that's an appropriate use of the time that we have. Okay.

We appreciate the commentary, Jim and we did, during the drafting process -- Jane and I, by the way, are the co-chairs for the ISE Privacy Guidelines Committee that is established by the Privacy Guidelines to conduct the ongoing dialogue that you're talking about and provide ongoing

guidance to the agencies as we implement these guidelines. I think you've properly described them as a framework. I would say that it is a very firm framework. I think there is meat on the bones here. We've certainly heard reactions during the drafting process, which was a very interesting one, where the concerns were raised that the guidelines would slow down necessarily information sharing and in fact, impose additional layers of bureaucracy and oversight. So we were dealing with those kinds of concerns while we were drafting these as well as trying to consult sources like the Markle Foundation report, which was very helpful when were going through the guidelines process.

One thing on the -- you mentioned the missions of the agencies -- that the U.S. Government is undertaking to clarify missions and roles through a variety of other efforts. So that is taking place outside of the context of the privacy guidelines and will obviously feed in here.

I think it is very important to keep in mind that the guidelines require agencies to conduct

themselves in accordance not only with laws but with their own missions and policies. So your statement about the purpose specification -- I know you haven't had a chance to review these in detail but there is actually a separate provision that says that the agencies can only seek or retain protected information that is legally permissible for the agency to seek or retain, under the laws and policies applicable to that agency.

We also require agencies to not only to do the kind of catalog for the data holdings that you're talking about but also access the rules environment in which they operate and decide if -- and document those rules, make any restrictions on their data holdings that are required by rules, make other agencies aware of it and put in place a process for ensuring that the sharing takes place in accordance with those applicable restrictions and as we anticipate that agencies, as they conduct those reviews, will find issues and problems and disagreements. The guidelines provide for those to be elevated to the ISE Privacy Guidelines Committee,

which will consist of the ISE Privacy Officials as well as obviously close consultation with the Privacy and Civil Liberties Oversight Board.

So I think that these are substantive additional protections for information, for privacy in the information sharing environment. Like I said, we try to refer to the work of the Markle Foundation and other groups as well as the fair information practices and principles. But you're right, it's a framework and we have actually budgeted for ongoing implementation support and guidance. So we expect, as we learn from agency experiences and from dialogue with the public and external groups, what issues and concerns come up. We have a mechanism in place to provide ongoing guidance for the agencies on this.

Ms. Jane Horvath: I just wanted to add two comments. As we were drafting these, the architecture of the information sharing environment was being determined at the same time so it was very difficult to develop guidelines when we didn't know the underlying architecture and we anticipate

working closely with the Board going forward in both their oversight capacity and in utilizing their expertise in these matters. So there probably will be an iterative process as the ISC is determined more concretely.

Mr. Dempsey: I think the point about architecture is an important one that -- from the Markle perspective, one of the most important privacy protections was the notion that information should reside on a decentralized basis with the agencies that created it and that I now see in the ISE implementation plan, although it was something being debated at the same time that -- and I know that your guidelines were finalized or almost finalized before that plan may have been finalized. But I think that there's a little bit of a lack of integration, I guess I would say, between your guidelines and the plan and that is not necessarily a bad thing but there has been a debate and I'm not sure the ISE implementation plan will fully resolve the debate -- a debate over what is information sharing. And there are some agencies who say

information sharing means give me everything you've got and I'll figure out what to do with it and maybe I'll you what I did with it and maybe I won't.

It's funny because I've heard Agency A complain about Agency B, saying give us everything you've got and then I've heard Agency B complain about Agency C doing the same thing to it. So if you read the plan, the plan talks about a decentralized distributed architecture or environment for information sharing, which is the information resides with the agency that collects it and you create mechanisms to find it when needed, without having wholesale dumps of data across the transom or wall or whatever metaphor you want to use.

I do think that going back to two of your points -- one, certainly on the question of will rules slow down information sharing? I think the notion that people function better when told there are no rules, do what you think is best, is just not borne out by human experience. People need rules to do the right thing. People told there are no rules and we don't like rules because rules tie your hands

and rules are bad things, which was a little bit of the rhetoric that existed post-9/11. I think we should be beyond that now, that one of the purposes of the rules is to make the information sharing possible by creating the environment so that people know what it is that they can do and what they can't do but if people are left uncertain, then you get one of two things. One is you get the cowboys going off and doing dumb things or you get people frozen up because they are afraid of being criticized later for doing the wrong thing.

Now on the missions question, again, right now every agency thinks it knows what its mission is. But I still think every day in the government, one agency will say about another agency, what do those guys think they're doing? And right now, I still don't think we have a clear sense of mission definition from the political top down.

Now of course, not deciding is deciding. So to the extent people have been allowed to launch their own data centers or their own collection activities or their own intelligence operations and no one has

said to them, don't do it, then in a way, that's a decision to allow a multiplication of collection activities. But that's not the vision of an accountable information sharing environment that I think the Act calls for.

Mr. Davis: Jim, we have some limits on time and I hate to interrupt you because Alex and Jane have done such an excellent job for us but just to be clear on the record, we as a board have had almost no input as a board, on these guidelines. We got started in March. Our Executive Director has done an outstanding job, Mark Robbins, in working with Jane and Alex. But as a board, we now look to our oversight function to get more involved in the substance of these guidelines. Some of us have been asked, well, what input did you have in the drafting, development, debate, controversies -- the answer is, very little because we got started so late. But we did have our Executive Director at the staff level involved and we certainly appreciate all the work that Alex and Jane have done in reporting to us. We were briefed twice about the guidelines.

But we look forward to getting into this in more detail when we are performing more of an oversight function.

Mr. Dempsey: I agree with that entirely.

Ms. Dinkins: Thank you to the panel. We appreciate your being with us.

Panel respond: Yes, thank you.

Ms. Dinkins: And we will take another question or two or comment from the audience while we move from Panel 2 to Panel 3. Again, if you don't have the opportunity, we encourage you to contact us as I had suggested previously, please.

Ms. Hoffman: I'm Marcia Hoffman. I'm with the Electronic Frontier Foundation. Based on the briefing you've received on the warrantless Surveillance Program, could you please tell us whether you think that program can be conducted consistent with the requirements of FISA or whether the program would be impaired if those who conduct the surveillance have to make applications for FISA orders?

Mr. Davis: If you're addressing that to me, I

think that the only way I can answer that is that Congress should be more involved in answering your question, reviewing the FISA law, the program itself and determining whether FISA needs to be amended. My uninformed impression is that it would be valuable for Congress to provide that oversight consistent with maintaining the secrecy that is inherently necessary if this program is going to be effective. So I don't think we or I could answer the question legally, whether FISA needs to be amended but I think Congress ought to be addressing that.

Ms. Hoffman: Just to be clear, my question is about the program with respect to FISA as it is right now.

Mr. Davis: And I don't know enough about the FISA law and its reach or scope to be able to answer. I know that what I saw, I was impressed with the individuals' concerns about privacy and civil liberties but I would like Congress to provide, as we heard in our earlier panel, more oversight.

Ms. Dinkins: Next question, please.

Mr. Bomrig: Hi, I'm Jared Bomrig. I'm a graduate student at the London School of Economics. Does the board have jurisdiction of oversight of the detention of Khaled El-Masri? And if not, could you please explain why your statute would not give you jurisdiction to do so?

Mr. Davis: You're talking about the individual represented by the ACLU?

Mr. Raul: Well, as I understood the question but then with Lanny's clarification, maybe I didn't follow it. But I understood it to be whether the board has jurisdiction over activities outside the United States, not applicable to U.S. persons? Is that the question?

Mr. Bomrig: Yes, in the specific context of Khaled El-Masri.

Ms. Dinkins: We do not address specific issues or cases like that. I would say specific cases. Thank you.

Mr. Bomrig: Can I just follow up with one other? I thought earlier that you guys had said you

will make recommendations concerning pending legislation in Congress?

Mr. Raul: That would be -- I believe that I may have responded to that question. We certainly wouldn't make direct recommendations, really, under the constitution, the power to recommend necessary and expedient measures to Congress is clearly assigned to the President under the Constitution. As part of our internal advisory function, it would be within our jurisdiction to develop views on legislative proposals and to provide that advice internally.

Ms. Dinkins: Yes?

Professor Weiss: I'm Charles Weiss. I'm a professor here at the Georgetown School of Foreign Service. I'd like to make a brief comment, if I could.

Another way of saying what the gentleman from the Heritage Foundation said, was that there really is very little law or jurisprudence on the subject of data mining. And for this reason, there's very little -- there are very legal or constitutional

limits on data mining. If you say it another way, once the information is out there, anybody can put it together in virtually any way they want as long as it's public. Now what that means is that the defense of privacy is basically one or another of the various forms of governmental inefficiency. The problem with this is multi-fold. First all of, it's very easy to aggregate information now. At the time most of these rules were put together, it was hard to aggregate information. Now it's easy to put together a profile.

The second thing is that there are very well established precedence that once you give information to anybody, it's out there and it's no longer yours with rather specific legislative, statutory limits. This 30-year old precedent has very bad consequences for privacy when put together with the ease of aggregation. And what this means is that the data mining is really an illegal no-man's land. There is very little jurisprudence on the subject.

So, in a sense, we're starting from scratch.

The various commissions and so on are starting from legal scratch and what this suggests is that the process that the gentleman from the Heritage Foundation, of judging the efficiency, the cost, whether there are less intrusive methods and so on, is a rather elaborate analysis of what the intelligence community really, really needs in order to its job and how it can be done with less -- with minimum intrusion. This is a problem both for the Congress and for the intelligence community because the intelligence community runs the danger of being whip-sawed if, as one always hopes, there are no terrorist events. Then people are going to ask, why are you being so intrusive about our privacy? And if there are terrorist events, God forbid, people are going to say, you had all these weapons! Why in the heck didn't you use them? So the result is that this is a much more careful analytic job than I think has been given credit for. Thank you for this few minutes, Ms. Dinkins.

Ms. Dinkins: Thank you, Professor. We will turn now to our third panel, introduced by our

member, Frank Taylor. General.

General Taylor: Thanks, Madame. Chairman, for the opportunity to introduce the panel and given the constraints of time and certainly in deference to the magnificent background of our panel, I'll be very brief in their introduction.

First we have Fred Cate, who is a distinguished Professor and Director of the Center for Applied Cybersecurity Research at the Indiana University.

Second, Peter Swire, who is the William O'Neill Professor of Law at the Ohio State University.

Third, we have Neil Katyal, who is Professor of Law at the Georgetown Law Center. And last but not least, our host for today, Anthony Arend, who is Professor of Government and Foreign Service at the Georgetown University. Gentlemen?

Professor Cate: Thank you very much, Ms. Chairman, Vice Chairman Raul, Members of the Board. It's a great pleasure to be here and I appreciate both your holding this public hearing today and the opportunity to be part of it.

You have my written statement. I would like to

spare you the pain of having it read to you and instead focus on five points, briefly, that are raised in that statement.

Let me begin by saying and I think this point has been made clear already -- despite the fact that many of the issues of which you're confronting are difficult and controversial. It is astonishing how much work has already been done about them. You've heard reference to the Markle Foundation Task Force. There have been many other conferences. There was the Technology and Privacy Advisory Committee in the Department of Defense. There is the Department of Homeland Security's Advisory Committee. What is striking about these is frankly, how consistent many of their recommendations are. So one of the underlying messages I would like to leave with you today is even as you grapple with the very difficult and controversial issues, there is a great deal of consensus about some of the basic things that need to be addressed and I encourage you to focus on those because frankly, the question on the table is why has there been so little action, action from

both the Administration and action from Congress on those steps that seem, if you will allow me, obvious, that ought to be done. And it is frankly on those steps that I would like to focus.

The first of those is recognizing that privacy and security, although we often like to refer to them as if they were somehow intention or an opposition, I think, in fact, really are consistent. I first heard this view presented when the TAPAC was holding its hearings and Noelle Conner Kelly testified as the Chief Privacy Officer for Homeland Security. She made this point and at the time I thought it was kind of that mindless government rhetoric that sounded good but in reality, could not possibly be right. How could privacy and security be consistent? But since that time, in the four years since then, I think we've seen demonstrated again and again, how often they really are consistent.

So for example, the principle and privacy that we care about, the integrity of data, that data should be accurate, that they should be relevant,

that they should be appropriate for the use, these were of course, all privacy principles. But I don't know anyone in the security community who would not think those were important security principles as well.

So when we see the government publishing its legally required Privacy Act notices and exempting its systems from these requirements, so that we are, in fact, going to base the TSAs online profiling system on information that is not relevant nor necessarily, it frankly raises concerns not only about privacy but it raises concerns about security as well.

Recognizing that we are not here, on the whole, in a balancing game, we are in a very consistent game of trying to achieve both. If I can just give one other brief example of that, one of the most common things that I hear government officials talk about when they have to go for a warrant or for an order from a court is the discipline it builds into the process. They are virtually never turned down for those orders. Courts routinely provide those

orders but it is the fact that you have to stop and get your ducks in a row and say, here's what we need and here's why we need it, it is that discipline built into the process that is perhaps one of the greatest benefits of those types of requirements.

Now second and obviously related to this, it seems clear that some form of external authorization or oversight or both are necessary, especially in the classified environment, as I think you are primarily dealing with today.

This is the guarantee that the public has. When we do not have access to the information that somebody else independent of the agency that is acting, will have access to that information. So whether that means oversight by this Board or oversight by Congress or oversight by courts or oversight by Inspector Generals or some combination of all of these combined, it is critical to use Marc Rotenberg's comment from earlier that the checks and balances be in place and be observed.

Frankly, one of the least explicable things that this Administration has done in its pursuit of

security-related database systems has been its unwillingness to use those checks and balances, to say, we don't have to go to a court. We're not going to report to Congress. We're not going to use the systems that are available. I don't mean to suggest there would not be value in other systems being developed but the systems we have provide a useful starting point for building in the type of independent oversight, this sort of second guess of uses of information involving privacy.

Third, redress. This has been mentioned many times today. It gives a media advantage of coming near the end to be brief about this. Redress seems, of course, the foundation of virtually any system that uses information. Paul Rosenzweig, when he was a Senior Legal Research Fellow at Heritage, that the only certainty in this entire field is that there will be false positives and you need a way to deal with false positives.

But to be honest, redress -- I think is more important even than just the concept of fairness or of protecting individual rights. Back to the

starting point, it's important because it is what makes the systems work better. This is, in fact, the foundation of many of our privacy systems for ensuring accuracy. The Fair Credit Reporting Act is a good example. There are very few legal requirements that the information in a credit report be accurate. But what we have instead is a guarantee that when that information is used in a way that can impact an individual, the individual gets access to the data and an opportunity to challenge it. That's where the guarantee of accuracy comes in. It comes in, if you will, after the fact and this is not merely a more effective way of achieving it, it is a more cost effective way of achieving accuracy. It seems critical to me that for any system, whether it is the TSA or some other system, to be put in place that involves using information about individuals, there must be some form of redress.

Now as Jim Dempsey noted, sometimes it will not be possible to give individuals access to the data but a redress system seems critical and I want to

particularly applaud your efforts over the fall to address redress. I could not think of a more important issue.

Fourth, and without being the slightest bit flippant about this, rationality really matters in this area. When you are using data that has the potential to invade personal privacy that has real consequences for the individual that those data concern, having a rationale system that serves a stated rationale purpose and is subject to appropriate rationale oversight, is an absolutely bedrock requirement. And in this area, frankly, we have the least -- it is with this requirement we have the least consistency that I can see, in the current published uses of information.

So for example, we have the requirement from Congress that we now have to present government-issued identification every time we board an airplane, even though we know, not only did all 19 hijackers have either falsely obtained or falsified government issued identification but also we know that that form of identification is ultimately as

weak as any form could be right now, for identifying ourselves. My students routinely use false ID for all manner of purposes, which I would rather not be describing, perhaps, on the record. Yes, my colleague here, who understands what it's like.

So we have merely taken a completely -- a requirement which had no effect and we've made it law so that we now have an irrational requirement being carried out. Perhaps the clearest example we have of this, although it does not immediately involve data. It may involve other forms of privacy, is the current treatment of liquids when boarding an aircraft. There is not a security expert in the world who does not believe that 32 ounces of liquid is sufficient to cause a plane to leave the sky. Thirty-two ounces of the right liquid in the right place will absolutely bring down an airliner. Yet we have a requirement that you put all of your liquid in a 32-ounce bag and then it's fine because somehow putting it in that bag will insulate it from being dangerous any longer. So if you put five terrorists on an aircraft, as we know

happened in the past, you've got a gallon and an extra quart left over of the liquid -- we are accomplishing nothing with this system. It is 100 percent irrational. It is security theatre. It is designed to make us think something is going on when in reality, nothing is going on. And the clearest evidence of that is the frequency with which the TSA itself avoids that requirement. I've watched more TSA agents explain to complaining people, often women because it involves bottles of perfume, usually, that if you just put it on your person, the metal detector won't detect it because they don't believe the requirement makes any sense either. We see this type of irrationality again and again and I include in my testimony and I want to just repeat. One colleague of mine at the law school was unable to travel when her name was mixed up with somebody else's on the watch list. I must confess, I'm assuming that she is not, in fact, a terrorist. So she did not, unfortunately, have the benefit of being Ted Kennedy, who had a certain degree of notoriety. She had to go through the

process, which was instituted late in the game. You submit four forms of notarized identification. You get a letter back saying please let this person travel. They of course, sent the letter back misspelling her name so that the letter has now been issued to the wrong person. This is the type of irrationality that undermines our system and it is very difficult to believe that it is reasonable to ask the public to give up privacy in the face of such an irrational system. It must be fundamentally rationale to start with, if you're going to say privacy, may in fact, have to be compromised for some reason, to serve it.

Finally just a word about the nature of the current legal structure. I'm aware you don't write law and that's a good thing. I would be giving you an entirely different testimony if I thought you were the authors of this law. But it is very difficult today to make much sense out of the law applicable in these areas, in part because the laws are very complex as many, many courts have noted, calling it a fog, convoluted, fraught with trip

wires, confusing and uncertain and these come, of course, from some of the laws' strongest defenders. But also because the law has been made largely irrelevant by technology. So for example, the Supreme Court's decision that records held by third parties are no longer protected by the Fourth Amendment -- I'm not sure it ever made sense. But today, when all of our records are held by third parties, it clearly doesn't make sense. It needs to be rethought.

Now, your job, as I understand, is not to write the law. But I do believe the challenge of the laws' irrationality in this area does add some additional burden or opportunity, as you may wish to look at it, to your task. One is that you're going to have look beyond the law. As many, many people have discovered, saying this project is lawful is no guarantee that it respects privacy. Just ask Admiral Poindexter. It didn't work for TIA. It was wholly lawful, no question about it. But it didn't carry the day when trying to justify its impact on privacy. It may also mean that you need to help

identify where the law might be improved or how it might be improved, a task which I think all of us on this panel have been actively involved in but you will certainly speak with greater authority than we will, even combined.

I stress this point about the law not just again because of the importance of protecting privacy and civil liberties but also because of the importance of giving clear directions to the people who have to carry out the law. My experience working with TAPAC and as I have heard you talk, I believe it is your experience in what you have seen thus far, is that the people carrying out these programs are well-intentioned. They are law abiding, they are well trained. They need to be given clear rules. They need to be given policies and laws and rules that make sense. The failure, as far as I can tell, is not on the ground. It's not at the implementation level. It's much higher up and it is at that level where I am hopeful and confident that you will be able to help bring some much-needed scrutiny and rationality. With that, I

thank you very much.

Mr. Swire: Thank you. To begin, my thanks to you for the opportunity to testify here today, at the first public hearing of the White House Privacy and Civil Liberties Board. I will briefly describe my background relevant to today's hearing, and then discuss a Due Diligence Checklist that I hope will be helpful to the Board as you participate in the development of government information sharing projects. I am currently the C. William O'Neill Professor of law at the Moritz College of Law of the Ohio State University, and a Senior Fellow at the Center for American Progress. I live in the Washington, DC area. From 1999 to 2001 I served as the Chief Counselor for Privacy in the U.S. Office of Management and Budget. If the title had existed at the time, I would likely have been called the Chief Privacy Officer for the Government. That title hadn't been made up yet. Most relevant to today's matters, in early 2000, I was asked by the President's Chief of Staff to chair a White House Working Group on how to update electronic

surveillance laws for the internet. And that was a big job. We introduced legislation. It was marked up that year but it didn't pass and those same issues came back the next year in the Patriot Act. So having worked through that, there are various scars on various parts of my body and so perhaps I'm trying to offer tidbits of insight or experience from that time.

And those tidbits are really crystallized in this due diligence checklist that is in my written testimony and is in the Lawyer View article that I burdened you with today also.

The core is this set of due diligence question for assessing information sharing programs. In many of my writings and many talks, I've stressed the benefits of information sharing. We have to use better IT, we have to get better at all these things. But the emphasis in due diligence is tempering the enthusiasm of the proponents. You know, in a take-over, you don't want to spend the shareholders' money until you've really checked what you're buying and due diligence forces people to

figure out what they are really buying.

When it comes to the peoples' data here, due diligence will force us, I hope, to check what we're getting into. How is the data going to be used? Are the proponents, who are all enthusiastic, who want to buy the thing, are they really -- have they gone through the process? Have they really thought it through carefully and asked the right questions?

I'm going to read the 10-point checklist and then make three quick points and close. The checklist is about policy. It's about what Fred Cate just called rationality. It's trying to ask the structured questions so you don't get blind-sighted. So I'll just read them quickly.

First, will the proposed information sharing tip off the adversaries? You don't want to help the bad guys.

Secondly, does the proposal really improve security? This is rationality. It is proposed to do something. Does it work and does it do it cost effectively? If it doesn't, you don't do it. It doesn't work on security and it doesn't work on

privacy, you don't do it.

Third is the proposal of Bruce Schneier and then Fred today, called security theatre. Is this an appearance of security thing or it is real security? You don't want to go build a program -- maybe it's worth having good theatre but you don't want to build a program pretending it works when you know it doesn't.

Fourth and I'll come back to this, are there novel aspects that propose surveillance and what goes with that?

Fifth, are there relevant lessons from history here? We've had histories of abuses. If we forget the history, we're condemned to repeat it.

Sixth, do fairness and anti-discrimination concerns reduce the desirability of the proposed program? If you do screening based on race, ethnicity, etcetera, there are certain issues that come up.

Seventh and this is not on everyone's list but are there ways the proposed measure actually makes security worse? That's a devil's advocate question.

If you sit and look at the proposal and then you say, is there any way this actually makes it worse? Sometimes you think of things and then they better have an answer or else they really don't deserve to go forward.

Eighth, what are ramifications internationally with other stakeholders? The agency wants it. Maybe three agencies want it. Who else has a stake here?

Ninth, are there other privacy based harms and we've heard a lot of Fair Information principles.

Tenth, will bad publicity undermine the program because it's not likely to stay secret forever?

So with that as a list and with the writing to get background, I'm going to highlight three points quickly and close.

The first topic on the list is whether information sharing tips off adversaries and think about watch lists here. Greater information sharing clearly helps if many border guards have the watch lists and they catch somebody. But giving it to lots and lots of border guards also increases the

probability that one bad guy will see the list and then they'll tip off the suspect and the suspect will get away.

In my own writing, I've written at some length about information sharing, about terrorist watch lists and such. A main finding of this model of openness and security is that information sharing is a characteristically difficult case. It helps the bad guys and it helps the good guys and that's why it's hard. We should not have a presumption that sharing is good. That's my sort of bottom line there, that I talk about at length in other writings.

The second item of my three is that it is important to identify the novel aspects of a proposed program and here I'll cite Edmond Burke and the conservative tradition and I have worked for a bunch of conservatives along the line and I could quote it to prove I really mean it but here I'll first quote Jude Wanniski, a supply side economist. He said, "Society is a vast and complicated historical product, which may not be tinkered with

at will like a machine. It is a repository of collective human wisdom to be regarded with reverence." And Hayek said, "The result of the experimentation of many generations may embody more experience than one man or even one agency possess." I added the one agency part.

This Burkian perspective is a useful corrective, I think, to the tendency to think that everything changed with 9/11. The conservative instinct suggests that some things changed on 9/11 but a lot of things didn't. And as a step in due diligence for proposed programs, it is useful to identify what is novel and consider the unintended consequences, consider what Hayek would say here, for instance. And the program should move forward if but only if the case for it is convincing.

The last of my three points are brief thoughts on the role of the Board in this new political context, now that the Congress has changed hands. During my two years in the White House, we had the privilege of having the other party control Congress. And this sometimes seemed to us that a

hearing would be called if someone hiccupped incorrectly. There was just going to be a hearing all the time. And that shaped our daily life of thinking about every sentence uttered and every word thought of.

This possibility of oversight, I think, suggests a particular and a heightened role for the Board in this slightly new political period. Proponents of programs within the Executive Branch perhaps have new reasons to talk very, very carefully and in depth with you, in the following sort of way. You have had this impressive list of contacts and learning with people around the Executive Branch, thinking about how these issues fit together, how to present them publicly. So when a proponent of a program comes forward, you have a possibility of saying something like this: Whatever my own views of the merits, here is what it is likely to look like in the Congressional oversight process when these privacy people come and testify and all the rest, let’s see how we can fix this program, how we can work with it, so it will hold up

very, very well to the new scrutiny that it is likely to be subjected to. And if we do a really good job internally, that's going to be good externally for the country. It's going to let us have better programs. And that's an internal selling point for the usefulness of the Board, to be brought in for legislative proposals, for program proposals and all the rest because hard-headed thinking and the experience you've developed is going to make the products of the Executive Branch better and better able to withstand scrutiny in this new environment.

So in conclusion, the due diligence checklist is an attempt to draw my own experience in government. We're trying to serve our nation by asking the thoughtful questions, being effective here. In this way, the proponents get a little bit of criticism inside so they do a better job for the whole program outside and when due diligence is done well, then the right deals are done and the other ones aren't. Thanks very much.

Professor Katyal: Thank you, Madame Chair and

Members of the Board, for inviting me to speak to you today. On November 28, 2001, I testified before the Senate Judiciary Committee about the President's then two-week old plan for military tribunals. I warned that Congress, not the President, must set them up and if Congress did not, the result would be no criminal convictions of terrorists and a court decision striking those tribunals down.

Eighteen hundred and thirty-three days have elapsed since that testimony. During that entire time, not a single criminal trial took place at Guantanamo nor was a single criminal convicted. It took more than two years before anyone was even indicted and on June 29th of this year, the Supreme Court invalidated this scheme. I did not come here to gloat. The decision to file this lawsuit was by far the hardest professional decision I had ever faced. I previously served as National Security Advisor at the Justice Department. My academic work extols the idea of the unitary executive theory of the presidency. My work in criminal law centers on the need for tough criminal laws to benefit

prosecutors and I come to this body today with a warning similar to the one I gave the Senate in November 2001 and I address it specifically to this Board's mandate at looking at United States persons. An unfortunate trend in recent United States policy after 9/11 is to create a crass dividing line with some United States persons, namely citizens, on side of the line and other United States persons, such as lawful green card holders and aliens, on the other side of that line. I speak today to address the rights of those other groups on the disfavored side of the line who don't have the opportunity to speak for themselves, either when they are detained on United States soil or at Guantanamo, which for all practical purposes, as Justice Kennedy said recently, is United States soil. So I'll concentrate my testimony on that area of law, which I know best, which is the detention and trial of suspected enemies of the United States, though I warn that there may be other areas in the United States law where that distinction between citizen and alien is being codified, perhaps even in the way

this Board views its mandate.

The government's recent attempts in the Military Commission Act and the President's preceding military order of 2001, that providing alien detainees with an inferior brand of justice, offends the very essence of equal protection under the law. Shutting our courthouse doors to alien detainees, both green card holders in the United States and foreigners and relegating them to military commissions sends the message that their rights are less worthy of protection than those of United States citizens. Yet everything about the Equal Protection Clause, from its plain text to its original intent, shudders at the notion that justice could be conditioned on citizenship. This is not a circumstance in which the government is handing out a goody, like a welfare benefit or a job. It touches the raw nerve of justice and it decides, for example, who will be put to death or not, on the basis of where their citizenship lies.

For me, my starting point are the words of Justice Scalia, who wrote, "Our salvation is the

equal protection clause, which requires the democratic majority to accept for themselves and their loved ones what they impose on you and me." Justice Scalia's words track those of Justice Jackson years earlier who said, "There is no more effective practical guarantee against arbitrary and unreasonable government than to require that principles of law, which officials would impose on a minority must be imposed generally, that nothing opens the door to arbitrary actions so effectively as to allow those officials to pick and choose only a few to whom they will apply legislation and thus escape the political retribution that might be visited upon them if larger numbers were effective." The force of Justice Scalia's and Justice Jackson's principles is at their height, when life and death decisions are on the line.

If Congress deems terror suspects too great a threat to warrant even access to the federal courts with the writ of habeas corpus, at a minimum, they must deny such access for all persons and not selectively target those without a political voice.

But that is what President Bush's now invalidated military order did and what the recent Military Commission Act now purports to do.

Indeed, this new act of Congress purports to deprive habeas corpus rights for all aliens, even lawful resident aliens, such as green card holders, who live in the United States. The framers of the Fourteenth Amendment would have rebelled at such a notion. If you look at the text of the Fourteenth Amendment, it protects not citizens but all persons.

Why did the framers of the Fourteenth Amendment use the word persons? Well, they did so for a simple reason. Representative Bingham, who drafted the Fourteenth Amendment, wanted to overrule the worst line in the worst Supreme Court case in American history, the line in Dred Scott that said that only citizens have constitutional protections. Representative Bingham said no, we fought a war against that idea and we protect all persons with equality on basic rights.

The disparity between aliens and citizens in the War on Terror presumes the former are more

dangerous, so much so that the confines of our constitutional protection cannot contain them. But our country knows all too well that the kind of hatred and evil that has led to the massacre of innocent civilians is borne both at home and abroad. The threat of terrorism knows no nationality. It is a global plague. Its perpetrators must be brought to justice no matter what their country of origin. Make no mistake, terrorism does not discriminate in choosing its disciples. If anything, we can expect organizations such as Al-Qaeda, whenever possible, to select American citizens to carry out its despicable bidding. There is simply no reason why the government must subject aliens to military commissions and shut the courthouse doors but need not do for citizens suspected of the same crimes. A citizen who commits a terrorist act is just as culpable as the alien who commits it. Indeed, there is an argument that the citizen's actions are worse, since he is guilty of treason on top of whatever else he has done. Laws of general applicability are not only preferable, they also keep us safer. In

affording the same process to aliens and citizens detainees, we maintain the superiority of our judicial system, the federal courts have a tried and true record that discerning the guilty from the innocent, our civilian courts have prosecuted the 1993 World Trade Center bombing, the Oklahoma City bombing, Aldrige Aimes, Manuel Noriega and dozens of other cases. Indeed, the Justice Department has recently extolled its success on the War on Terrorism, talking about over 500 prosecutions, successful ones, in our criminal courts in the United States.

Finally, in the wake of the international disdain for the military tribunals, our country is already under global scrutiny for its disparate treatment of non-U.S. citizens. We must be careful not to further the perception that in matters of justice, the American government adopts special rules and special boards that single out foreigners for disfavor. If Americans get a Cadillac version of justice and everyone else gets the beat-up Chevy, the result will be more international condemnation

and increased enmity by Americans worldwide.

The predictable result will be less cooperation, less intelligence sharing and fewer extraditions to boot.

In sum, in splitting our legal standards on the basis of alienage, we are, in effect, jeopardizing our own safety and our national interest. When United States terror policy is driven by anti-alien sentiment, the result is only our own isolation. It will lead to a chilling of relations with key allies abroad and it will also alienate many of our own citizens, who have relied on our country's longstanding commitment to equal justice for all.

I ask this panel to remember the words of a great American patriot, Thomas Paine, who wrote, "He that would make his own liberty secure must guard even his enemy from oppression for if he violates this duty, he establishes a precedent that will reach unto himself."

Professor Arend: Madame Chair and Members of the Board, as I said at the outset, it's a real honor to have the Board here at Georgetown

University for its first public session. It's an honor to be here testifying before the Board and to be once again with my colleague, Neal Katyal. I'm also extremely cognizant of the time and as a consequence, I'll attempt to be very brief in my remarks. Hopefully everyone has a chance to look at my written testimony but what I really want to do is talk a little bit about the NSA Surveillance Program. It's been something which a number of speakers have referred to and Mr. Davis in particular, has raised some interesting questions about FISA and about the potential for amending FISA. So it's in that context that I want to address three questions, briefly.

First, is the NSA Surveillance Program constitutional? My short answer is, it's completely inconclusive. It's impossible right now to make a final decision on that and I'll play us through the case law on that.

Second, does the FISA framework nonetheless remain the best framework for regulating the NSA Surveillance Program? My answer is decidedly yes.

And third, that being true, how can FISA be changed? How can it be amended to accommodate that program? And I'll have some suggestions, understanding that you all are not writing the law but at least it puts some suggestions into the process so that can go for further deliberations.

First of all, the constitutionality question. I wish I could come here and say, I am absolutely certain that this particular program is constitutional. When Neal Katyal made reference to the President's Military Order, I was confident that that was unconstitutional but I can't say the same thing about the NSA Surveillance Program, for the following reasons.

First of all, the Supreme Court has never pronounced on whether the President can authorize surveillances in response to a foreign threat to national security without a warrant. In 1972, in the so-called Keith case, *U.S. v. U.S. District Court*, the Supreme Court said if you have a domestic threat to national security, you need a warrant. But the Court explicitly said we are not pronouncing

judgment on whether we would need a warrant for a foreign threat, a threat posed by foreign power or the agent of a foreign power. So it left that undecided. So we have no Supreme Court precedent on this question.

Well, if we look at the lower courts, what do we see? We see, in my view, no clear jurisprudence there either. One of the cases that is often cited in support of this, is *U.S. v. Trung Din Hung*, which was a Fourth Circuit case from 1980. In that case, the court clearly said the President had constitutional authority to conduct surveillance without warrants when you're dealing with a foreign threat to national security. The case was decided in 1980 but the incident occurred before FISA had been adopted. So I'm not sure what we can get out of that particular case.

Another case that is often times cited in support of this is a decision of the FISA Court of Review, from 2002, the so-called En Ray Seal Case, 02-001. In that case, the FISA Review Court said, we take for granted that the President has the

authority to conduct these surveillances without a warrant. But that was dicta. So we don't even have the FISA Review Court squarely holding that the President had that authority. So those are the constitutional side cases.

On the other side, there are some suggestions that it may be unconstitutional. *Wybon v. Mitchell*, for example, is cited, a 1975 D.C. Circuit case. But in that case, we have a plurality opinion of the court, where the court says or the plurality says, in dicta, that it's unconstitutional for the President to conduct such surveillances. So that doesn't really, in my view, help us.

Then we have *ACLU v. NSA et al*, which was decided by the Eastern District of Michigan a few months ago. I have read this case and I really see no discernable legal principle coming from the case, in all due respect to the judge. But as I look at the case, the court says -- and this is a District Court. The court says, the NSA Surveillance Program is in violation of the Fourth Amendment and the First Amendment. But when I look, in particular, at

the Fourth Amendment analysis, the court doesn't engage these cases I mentioned. It doesn't make an argument about the nature of presidential power. It doesn't argue about what reasonableness would be under the Fourth Amendment so as I read the case, I'm left scratching my head, saying I really get no jurisprudential guidance.

So at the end of the day, my conclusion is, I can't tell you whether it's constitutional or whether it is unconstitutional. I cannot make a clear argument on one side or the other, which leads to the second question.

In light of that, does FISA remain the best framework for regulating the NSA Surveillance Program? And I think the answer is clearly yes and here's why. As I understand it, when FISA was concluded in 1978, the purpose was to establish a compromise between the President and Congress. In FISA, the President did not renounce - -this is President Carter -- President Carter did not renounce constitutional claims. Rather, the President and the Executive Branch said we're going

to bracket those claims. We're going to keep them out there but what we're going to do is, we're going to agree to bracket those claims in exchange for a workable framework, which will allow us to conduct these surveillances, which will provide for some form of judicial scrutiny of the type where the information can be secured and we can assure that this will not be leaked out and get beyond where we want it to go.

With every account that I've read, this process has worked extremely well, at least up to the recent NSA Surveillance Program. My feeling is the logic that made FISA workable in 1978 still applies today. It is far better, in my view, not to push to a constitutional crisis between President and Congress on this issue. If we can continue, bracket those ultimate constitutional questions. Continue to hold them in abeyance but put together a workable framework -- I think the country will be much better off than if we had tried to push to those ultimate claims of presidential power.

Now based on that, my third point is I believe

FISA can be adequately amended. I know there are a lot of proposals that are circulating through Congress. Senator Specter has drafted several bills which seek to do this.

I have a modest suggestion -- nothing set in stone here but some ideas which I would want to throw into the mix as a possible framework whereby FISA might be adopted to deal with the NSA Surveillance Program and just in short, my suggestion is that the FISA Court be authorized to issue orders to monitor electronic communications between a U.S. person located in the United States and a foreign power or agent of a foreign power, provided it can be established to the satisfaction of the court that -- and four requirements. Once again, not set in stone but something to talk about, something to put in as grist for the mill.

One, the U.S. person is engaged in regular communication with a foreign power or agent of a foreign power. The idea of regular communications is not someone who has made a random phone call or sent a random email but there's some evidence which

the court finds to indicate that there is regular communications.

Two, the foreign power is hostile to the United States as determined by a Congressional Resolution or a specific presidential finding. So we're saying whatever the foreign power is, is the type of person, the type of power we concerned about.

Three, the information sought from this monitoring is necessary for the protection of national security of the United States and cannot reasonably be obtained from some other method. There is always going to be a preference to look at other methods so I think a certification that this is the way we have to go to get the information is critical.

And finally, none of the information obtained through this monitoring will be used in any criminal or civil proceeding against any U.S. person. If the purpose is for intelligence gathering as opposed to criminal or civil litigation, I think we need to spell that out.

Something along these lines, something more

detailed, something dealing with these issues, I think, can be done and I would urge this Board and others considering it, to move forward because I continue to believe that FISA is the best framework and by putting the NSA Surveillance Program within FISA, the country will be better off and I think the international system will be better off.

Ms. Dinkins: Thank you. Questions from the Board?

Mr. Davis: I have a question for Professor Katyal -- is that the right pronunciation? First of all, I was very impressed with your testimony and I appreciated the legal research you did. At one point, you say concerning the political implications of making the distinction between non-citizens and citizens, in the wake of international disdain for military tribunals authorized by President Bush in his military order, our country is already under global scrutiny for its disparate treatment of non-U.S. citizens. We must be careful not to further the perception that in matters of justice, the government adopts special rules that single out

foreigners for disfavor. In looking at the mandate of this Board, which is to be concerned about privacy and civil liberties, would you have us limit ourselves to U.S. persons or does it raise the same implications that if we're concerned about U.S. persons' privacy and civil liberties rights, we're making a distinction if you don't happen to be a U.S. person, we're not going to be looking at those issues as a privacy and civil liberties board. What is your recommendation on that?

Professor Katyal: My very strong recommendation is that you look at both United States persons and others. I don't think that you are barred as a board, from doing more and indeed, it's necessary and integral to the function of this board because if our policies give certain benefits only to what we call United States persons and no one else, it will have dangerous consequences. We're already starting to see those consequences. Britain has negotiated certain side deals with the United States for treatment of its detainees, more like what the Americans get. The rest of the world

is incredibly upset about this. You go and Australia, for example, is really upset with the idea that their detainees are still at Guantanamo but not others. I think it is impossible to really effectively look at the War on Terror without examining the this fundamental question, if for no other reason than it makes just good legal sense because any policy which discriminates or treats United States persons differently than other persons will be subject to the challenge in court. And I think none of us really want that. Instead, it would be much better to get policies that are going to stand up in court and produce convictions and produce the intelligence information that we'd all like to see.

Mr. Raul: For Professor Cate. Fred, you mentioned and I think referred to Jim Dempsey's point about redress, alternative redress mechanisms where the individuals do not -- may not be able to access the information that is held about them and perhaps an alternative, I think you said system of redress. Do you have any concrete ideas or

suggestions in that regard for us or have you written articles or books on that subject? Or where can we look to for your thoughts there?

Professor Cate: I do have some concrete suggestions if by concrete, you mean specific and not just weighty and useless.

Let me say, I don't think there are any easy answers here and I don't want to remotely suggest that there are. I think the issue is that the fact they are difficult is no reason to say we can't do it. We're just going to use inaccurate information and hey, so be it. So one thing is, we need to draw brighter lines about where does it really not matter if the person is given access to the information or is given knowledge about the basic source of the information. I would guess in most cases of say, TSA screening, that would be true, that telling Ted Kennedy why he is not allowed on the plane is probably not going to be a major threat to domestic security so we've created, if you will, a classified environment where none is necessary. That's really more -- I would guess -- I have been told, an

identification issue rather than a value of the information and so there, we need to confront the fact and this comes back to the rationality point, we are doing something that is fundamentally irrational. You know, most businesses can't identify people accurately, given all the data in the world about them. What makes us think, given an intelligence intercept from a cell phone call, where we got part of a person's name. We've added them to a watch list and we're going to match that with someone who shows up at the airport? So we're trying to do something which is fundamentally probably not capable of being done. In areas where we would say yes, it is possible to do it and it is truly classified, then the question becomes, first of all, can you use attorneys who have clearances? So if we can tell the person they are being blocked. We're doing the surveillance. You're not being allowed but I can't let you have access to the data. Why not have people with existing clearances to handle those cases, as we do in other national security areas, rather than say, well, sorry. You

just don’t get any redress at all because it’s hard. We don’t know how to do it. Instead say -- you know, I can see this as an ABA project today. So you’d have 100 pre-cleared lawyers who would take these cases.

In other areas, it may be more categorical information is what’s needed, that they don’t need access to the actual specific data. It may obviously turn on what the consequences of the data -- in other words, saying to someone, you may be subject to extra search at the airport is different than saying you cannot fly or saying, we’re going to put an Air Marshall next to you on the airplane is different than saying, you cannot fly. So it may be that it requires us to have a broader range of options for what we do as a result of having a positive match in the data rather than just these sort of binary choices that we seem to be currently stuck with.

But let me say, there’s a lot of work that’s been done on this and not by me. I mean, by many other organizations. This is not a case where the

wheel needs to be reinvented. Rather, someone -- you all, I hope -- need to put your hands around it and say this is what makes sense. These really don't. These don't but we can work with these.

Mr. Olson: Professor Arend?

Professor Arend: Yes?

Mr. Olson: Your fourth point about the change that you would do with FISA with respect to this, none of the information obtained through this monitoring will be used in any criminal or civil proceedings against any U.S. person. FISA as it is presently constructed and used, permits the use of information in a criminal proceeding. There are two parts to my question. One, I guess you would -- would you change that? The second part is, if you do follow this mechanism, this procedure that you recommend and you obtain evidence as a result of a FISA warrant, that contains lots of evidence of criminal activity, in fact, an ongoing criminal conspiracy or blow-up San Francisco or something like that. What would you do then? I mean, one of the way to protect against terrorism is to go and

capture the person and then prosecute the person and would you just let it go? Would you then transfer it to a different type of warrant? Would you use the information to get another type of warrant? Where would you go with this?

Professor Arend: My sense would be to do exactly what you just suggested -- use that information to get a different type of warrant, to get a regular Title III, if you're doing electronic surveillance or whatever type of warrant that you would normally get in a criminal investigation so that you pull that out of the process.

Mr. Olson: You mean start over again with a different warrant? I mean, this is an ongoing, active plan to blow up San Francisco. And you go back to a different judge with a Title III warrant and hope that you get the same information?

Professor Arend: No, I take your point, Mr. Olson. My sense would be if it were that critical information, you would be able to get it. If it really were information of that level, you would be able to get it. Having said that, I can certainly

understand where there would be debates on this. That's a point that as I was preparing for this, that's a point that I'm feeling extraordinarily strongly about but what I was trying to do is differentiate this type of program from the other aspects of FISA and I was trying to put a slightly different level of scrutiny on that.

Mr. Olson: Well, I know we don't have time. I have some other questions. I think it's very interesting and it's something we're probably going to want to talk a lot more about. So --

Professor Arend: I would certainly be more than happy --

Mr. Olson: Yeah, we may well be in touch with you.

Mr. Swire: Just a sentence or two on FISA, perhaps? The first panel was asked what changes in FISA would you make. I've been in debates recently on FISA. There is one issue that I think is the hard issue that I'm able to see, which is at the initial moment, you don't know if a person is linked to a foreign power or not and you don't get all the

way to probable cause until you've bootstrapped it somehow. You all get classified briefings that the rest of us in the world don't get and so you might be able to be considering if that's really the problem, then what are the tricks, the legal ways you might address that box? And having been through a number of debates, that's the legal change area where I'd hope the people on the inside, with the classified briefings, can be thinking about what you do in that initial stage, when you think maybe reasonable suspicion, a link to somebody. But you don't have enough to prove probable cause. That's the hole in FISA currently that I've seen that needs the most attention.

Mr. Davis: Peter, could I just say that you've asked the right question.

Mr. Swire: Hurray! Good.

Ms. Dinkins: Given the lateness of the hour, we will unfortunately not be able to take questions from the audience but perhaps one or two of our members could stay and chat with you if you have something you would like to raise. I also would

like to thank our other staff, Seth Wood, here in the front and Mark Robbins, our Executive Director, for all their hard work and I introduced John Coghlan a little earlier. We appreciate very much all your efforts to organize this. As you can see, we're testing our format and we will, in our next public meeting, be able to adhere hopefully to the schedule more closely. We thank the third panel and all of you for being here and particularly thank Georgetown for having us.

[Applause.]

[Whereupon the hearing was adjourned.]