Department of Homeland Security
Data Privacy and Integrity Advisory Committee

OFFICIAL MEETING MINUTES

Wednesday, September 28, 2005
Hotel Bellwether
One Bellwether Way
Bellingham, Washington 98225

AFTERNOON SESSION

MR. ROSENZWEIG: I call the meeting back to order. The first item of business in the afternoon, before we get to the afternoon panel -- which I might add, I personally am looking very much forward to -- is the report of the subcommittee. We skipped two this morning, which we may or may not get to, but since those subcommittee reports are more in the nature of progress reports than items for consideration, if we skip them, it won't be a tragedy, though it will be less information.

But the first item in the afternoon in the subcommittee reports is a report from the Data Sharing and Usage subcommittee that has prepared a nonfinal draft for consideration of the Committee, which, if approved, would be for transmission to the Chief Privacy Officer and the Secretary of Homeland Security.

So with that, David -- all the members have had a chance to review and comment on the draft in the ten-day reading period beforehand. If you would, for them and for us, identify the subject matter of the report and a short précis of it so we can have a public discussion.

MR. D. HOFFMAN: Thank you, Paul. I believe that copies of the report have been made available. They have been made available on the table on the outside of the room.

The report is about the issue of use of commercial data to reduce false-positives in screening programs. I'd like to particularly note that this is a collaborative effort from the members of the subcommittee. Several members of the subcommittee came together and spent significant amounts of time putting this report together, and of that, I am extremely grateful. I am also grateful to those members of the overall Committee who took the time

to review and provide comments, which I believe have actually made this a much stronger and more beneficial report.

I would also then like to say, our intention, as a subcommittee, and hopefully the full Committee, is to adopt this and then to ask any of the public -- any of the folks in the public who would have additional comments or reactions to this or questions, to submit those comments, and those questions and/or comments can be submitted through the Committee's website through the Department of Homeland Security, and we will then take those into consideration. And all of those comments along with this document will continually be made available at that site.

So I mentioned the title of the report. The scope of this report was to look at some broad overall issues that are associated with the activity of when commercial data would be used to drive down false-positives in screening programs. I think if anyone wants more detail on exactly what we mean by any of those particular phrases, we tried to define those in the document.

We are expecting that this document will be a building block for further discussion on the overall issue of the use of commercial data, and several members of the subcommittee have expressed substantial interest in continuing our analysis and taking some of the points that were raised in this document and building on those in much deeper analysis.

I would also like to note that the paper does refer to the Secure Flight program. This is not a review of the Secure Flight program. It is used as an example only to flesh out some of the overall broad principles. I would like to, though, state that -- in line with comments that were made earlier today, that the folks with the Secure Flight program have been extremely forthcoming in helping us get any information that we might need to fully flesh out the issues.

So I would like to, then, just give a brief overview of the structure of the document and our overall conclusions, and then we can open it up for any discussion we need to have. What we did is, we broke this out into some key areas that we thought were implicated by the use of commercial data for the specific purpose of individuals who have been identified by a screening program and that some consequence happens to them as a basis of being identified and that the commercial data could reveal that it is not the individual that people are trying to identify and, therefore, it is a false-positive.

The first section we dealt with is, we actually wanted to ask a number of questions about the commercial data itself, specific questions around data quality, how the aggregation of the data happens, does that then make the data more sensitive, and are there less sensitive or potentially less intrusive data elements that could be used to serve the same purpose.

The second topic we wanted to look into was access, so if the data is going to be used, to try to reduce the number of false-positives; how can access be limited so as to mitigate any risk that might come up.

And, third, we wanted to do what I think is a fairly lengthy analysis on use, disclosure, and storage. I think one of the areas that the subcommittee thought was critical was an understanding of what is the specific purpose that the data would be collected at or brought into the government or used in some capacity and making certain that we understand what really is the potential harm that that use is trying to mitigate and understanding, if we are going to run risks from accessing that kind of data, that the harm is strong enough -- that it is enough harm that it actually warrants taking those risks even if they could be mitigated in any other ways.

Then we also looked into practical issues around disclosure and storage, whether the data would be disclosed to other third parties and what mechanisms would be put in place over both the security that would be provided for the data and then also what the retention period would be for holding that data.

The fourth category that we looked into was transparency and data subject access. The subcommittee felt strongly that it is critical for the Department of Homeland Security to engender trust with individuals both within the United States and outside of the United States, and a key way to do that is to make the system as transparent as possible, both the system itself and providing an opportunity for people to be able to access data if that's appropriate and does not frustrate the security efforts that the Department of Homeland Security is trying to accomplish.

The fifth section of the paper is on regulation and redress, and this was an important conclusion that we came to. In line with the earlier comment about engendering trust through transparency, there -- Under the Privacy Act of 1974, there are a number of exemptions that are provided. We thought it was actually very important for people who are part of DHS to not take advantage of those exemptions, even if they do qualify for them in a certain situation and subject themselves to the rigors of the Privacy Act in order to help engender that trust.

We also looked into the issue of redress, and to further engender that trust, we think it's very important for DHS to focus on not only providing a mechanism for people who are identified to try to show that it is potentially a false-positive but to actually make sure there is a high degree of awareness as to what those procedures should be and that those procedures are simple and easy for people to be able to take advantage of.

The last point that we looked into were alternatives. We wanted to make sure that for every analysis there always should be a part in the process to look and to see: Are there less intrusive ways to accomplish the same purpose. And I do want to make clear

that this paper is not an articulation of specific alternatives that were recommended. Instead, we did -- We have some alternatives in here. They have not been tested in any way. There could be unintended consequences from them. We use them only to demonstrate the fact that there are other potential alternatives and others ought to be -- DHS ought to take the time to see if there are others that could be explored.

So very quickly, I would like to describe the final recommendations that the paper came to, which are listed on Page 14 of the paper in the bullet points. And what we found is that for the issue of use of commercial data for false-positives, at least -- and we're going to take a look at these and see if these apply more broadly -- the following recommendations we thought we would like the Committee to adopt and we would like DHS to adopt when looking at this issue.

Number one, the necessity to satisfy a defined purpose and to minimize processing just to that individual purpose and to make sure that that purpose is narrowly construed, instead of broadly.

Second, to make sure that data quality issues are analyzed and satisfactorily resolved.

Third, to find that access to the data is tightly controlled.

Fourth, that the potential harm to an individual from a false-positive misidentification is substantial. We thought this was a very important point, and we think it's due for a lot more analysis, to actually see, really, what is the degree of harm that happens to an individual from these misidentifications.

Next, that use for secondary purposes is tightly controlled, transfer to third parties is carefully managed, and robust security measures are employed.

We also then, in the area of data retention, recommended that the data should only be retained for the minimum necessary period of time to accomplish that specific, defined purpose, and the overall issue that transparency and oversight are provided. And we already talked about a couple of the specific recommendations for that.

That the restrictions of the Privacy Act are applied, regardless of whether an exemption may apply; that simple aspects of redress is provided; and that the less invasive of the alternative is exhausted.

So, Paul, I'll turn it back to you.

MR. ROSENZWEIG: Thank you, David, for that summary, and I want to begin by thanking the subcommittee for what I think is a very productive and excellent effort. This is obviously the first of many products that will come out of this Committee, I hope.

I hope. Right, guys? Many products of that Act are intended to be of use and to fill our advisory function.

I can speak to the paper, but before I do, are there members of the Committee who want to speak publicly to the paper and its content? So raise your tent card now, or forever hold your peace.

COMMITTEE MEMBERS: (No response.).

MR. ROSENZWEIG: Wow, that's good. I think that it's a great first step, and I would add that, in my judgment, the single most unique recommendation in there is the idea that, at least in the context of commercial data, where Privacy Act exemptions may exist, that we permit the Department to act irrespective of those limitations, that our recommendation is that the Department forego those exemptions or presumptively forego those exemptions as a means of trust. I think that's an important contribution to the discussion.

Howard.

MR. BEALES: I was struck by the point in the recommendations about potential harm to an individual is substantial. And I would just note that that -- I think it's important to be careful about that because it's -- obviously, we've got to think about proportionality. There's a privacy and intrusive approach here, and that shouldn't be used if we're trying to avoid trivial consequences to the individual. But I guess probably what the main point is that consequences that are trivial that only happen once are more significant if this is going to happen repeatedly. But the substantiality can occur that way as well.

MR. D. HOFFMAN: That's absolutely right, Howard, and I should have included that in the summary. But we actually mention that in the paper. So you're absolutely right, and I'm glad we got that on the record.

MR. ALHADEFF: Also, to further that point, one of the things that was stressed in the paper is the need to actually find more user-friendly in streamline fashion -- to make sure it doesn't happen multiple times. You know, the one time is understandable, but multiple times, there should be ways to prevent those. Those are not necessarily just technological ways but also practical ways of, "How do I actually complain about this fact, that I've been falsely identified?".

MR. ROSENZWEIG: Other members? Lisa.

MS. SOTTO: The one thing Joe just raised in my mind is, this is the first time I have heard about the Redress Office. Some of you may be familiar, but I think it's very important for us to understand what that office does, not only in the context of this paper but in the context of other papers we'll be writing.

MR. ROSENZWEIG: I think I can make the commitment that at sometime in the nearish future, probably December or March, we're going to be hearing from the DHS Redress Office. That's on my wish list.

Joanne.

MS. McNABB: I was intrigued in your paper with the idea -- the redress option of allowing somebody who does get an apparent false-positive of having the option of being able to permit the agency to consult commercial data in order to help clear them. That's kind of a novel idea.

MR. ROSENZWEIG: Going once. Twice. Okay. Well, our new bylaw was adopted yesterday and announced this morning. I don't need a motion and second, because that's kind of formal. So at this point, I'd ask for a vote on the adoption of the report of the subcommittee as a report of the full Committee from this Committee to the Privacy Officer, our sponsor, and the Secretary of Homeland -- John?

MR. SABO: Based on what David said, it sounded like if we adopted it, it would still be open for editing, based on public comment. Would you clarify that?

MR. ROSENZWEIG: Actually, that was perhaps a slight confusion. We are going to take public comments -- we're very interested in them -- as a means to building onto the next paper. This one is kind of in and of itself, and David's subcommittee has work to do, building upon that. But this is in and of itself.

MR. D. HOFFMAN: Let me just add to that. We do recognize that over time we may find that some of the conclusions in this document no longer hold, and if we do find that, through either comments or through our own analysis, I think we would probably revise the paper and do another version and have both.

MR. ROSENZWEIG: As we've experienced in many other situations, this is also for us an interim process, so this is a first step, but it is a step complete in and of itself. The only thing between here and transmission would be -- well, we're going to take another edit through it to make sure that all the grammar is correct and the tenses are right and the plurals match and singulars and such. But other than that, this is the report that would go forward.

Lance.

MR. L. HOFFMAN: As somebody who's been stuck with running some publications here too many times in the past, I might suggest that you consider giving this a number and serially numbering these things. It makes it easier down the road if there are going to be several, so people can refer to Report -- whatever -- 2005-01, or however you want to do it.

MR. ROSENZWEIG: That is fantastic, and I am going to designate this report 2005-01 of the Committee. And that will be one of the editorial additions that will be put into the final document before it is transmitted.

Any other questions or comments or... Well, then at that point, all in favor, say aye.

COMMITTEE MEMBERS: Aye.

MR. ROSENZWEIG: Any opposed?

COMMITTEE MEMBERS: (No verbal response.).

MR. ROSENZWEIG: Hearing no objection, the report is adopted. With our thanks, David.

Joanne, how much time do you need for your thing?

MS. McNABB: 15.

MR. ROSENZWEIG: Okay. So then I can give 15 to the other two subcommittees. Okay. Then I will be able to achieve that. Then I would call, the first one, Howard, to give a five-minute report on the activities of the screening subcommittee, just to update the members of the Committee, and as much of the public is going to read the transcript.

MR. BEALES: We have been quite busy and we have an ambitious plan, I think, but one that I hope is doable. We got back -- When we met in Boston, we had planned to do inventory screening programs. We had backed the information from the Department -- well, the known screening programs, in order to do that -- and we will turn that into a report that we expect to present to the Committee as a whole next time, once we can figure out some coherent organizing principles and make sure it's well-represented.

But the heart of what we're doing is looking at Secure Flight. Since we met in Boston, we've had several different meetings of all or part of the subcommittee with key people in DHS and elsewhere about the program in order to find out more details about how it works. And we had a very productive meeting yesterday to map out a work plan for how we're going to do this.

We're going to focus first on purposes, and sort of seeing the core purpose is finding people who are on the No-Fly list and then thinking about other purposes and what we know about those other purposes and what other purposes -- how we should think about which other purposes would be appropriate and how DHS should decide, and we would talk about that in the report.

We will look at a number of implementation issues in trying to assess the program. We will look at security issues in the system itself. We will look at security; in particular and more generally, the process of communicating with the airlines and disclosure back to the airlines of the results of a match or a non-match. We will look at the redress

mechanisms as to how people who are inappropriately false-positives can avoid that repeated fate. We'll look at the retention rules for how long the information is retained in the system.

We will look at the data that DHS is planning to collect, both at the level of data fields that would accompany airlines and data sources, as in the appropriate role or should there be a role for commercial data in the system.

And, finally, we'll look at the approaches to matching and the matching algorithms and look at the process that they're using to try to pick one and build from there.

We have an information-gathering phase and then we're going to have, obviously, some drafting and we hope to have a draft report when we meet again soon.

MR. ROSENZWEIG: Anybody with any questions for Howard?

COMMITTEE MEMBERS: (No verbal response.).

MR. ROSENZWEIG: Charles, tell us about the Emerging Applications and Technology subcommittee.

MR. PALMER: Well, that's the first question, which is to determine whether it's Applications and Technology or Technology and Applications.

MR. ROSENZWEIG: I like EAT.

COMMITTEE MEMBERS: EAT.

MR. ROSENZWEIG: But not ETA, Emerging Technology and Applications. But either way...

MR. PALMER: So good afternoon, public, speakers, colleagues, Committee. The subcommittee has been studying how we will prioritize our studies of technologies and applications. Clearly we realize going into this that DHS itself has large groups of people who are charged with deep evaluations of technology. We are not setting ourselves up to replace that function whatsoever. Perhaps to provide additional work, ideas, suggestions. There is so much to look at, and there are only a few of us on the Committee, so one of the things we started in Boston and continued in the interim was to try to determine how to prioritize, how we were going to go after these things.

Proposals were made. We pursued some of them -- one of them to the end, and we found -- Well, it involved identifying the key privacy concerns across the board for technology things, like openness and individual participation, data quality, updates, and so on. And then we were going to be very geeky about it, as you might expect from this subcommittee, and have each one of the members from the subcommittee provide priorities or scores for each of the technologies.

Sounds like a reasonably straightforward idea, except when you sit down to do it, you find it's akin to choosing which of two children you love the most. Not wanting to make such decisions, we decided perhaps that's not the best way to proceed. So as my thesis advisor told me, negative events are also a good thing to present; they certainly need to be resolved.

What we decided to do is to discuss the technologies along with the members of the Committee and come up with our ordering based on those discussions, which is what we would have to do anyway since all of the scores were coming up the same.

So...

MS. McNABB: Were they good or bad scores?

MR. PALMER: Well, they were all evaluated immediately. So if you want to know a specific that did appear at the end of the meeting at this time, our RFID, even without the benefit of our knowledgeable speakers today, it wouldn't be our first point of attack, and I think that would certainty be the case.

Now, we will also be contacting our DHS colleagues and Science and Technology directorate (S&T). I understand that one of the investments they plan over the next four years in technology -- not that we won't to do any budget diving, please, but what we're interested in is what do they think is an important technology and direction, not only to give us guidance as to what to think about but also to provide us with the opportunity to give them guidance back, saying, "Gee, that's not too good. Maybe you should think about that" or "Maybe you should think about this other thing or change the order" and so on.

So we hope to get that information as soon as we can, perhaps in a couple of passes going to the S&T, sitting in a chatting room, rather than trying to conduct this through e-mail, which is not that good a channel.

Finally, we will be continuing to work with the frameworks of the Committee to basically come up with some guidelines which we wish had been in place for some time, and that is, when you choose to employ or depend upon a technology, what is the thought process you should have gone through before choosing it, involving not only the issues of cost and availability and whether a subcontractor can do it or not but things like "Are they appropriately bounded from the beginning?" "Does the technology do what you ask it to do?" "Will it continue to do that going forward, and will it play nicely with other technologies that it might find itself surrounded by in the future?" Finally, we decided that we enjoy each other's company so much that we're going to meet monthly, in person, most likely in D.C. And maybe that isn't going to help us move a little bit quicker, but it certainly will be more interesting discussions.

MR. ROSENZWEIG: Anybody with questions for Charles? Joe.

MR. LEO: I just wanted to get the chairman on the hook for what I've asked for and which you've promised to review and look at, which was some of the members may think the agenda of our subcommittee is sort of long-range by looking at, for example, science and technology programs over the next four years and where they're going and so forth. And I've tried to wind the energy inside me wanting to say things in realtime on real technological issues that the department may or is currently facing.

An example would be if they made an announcement on a TWIC card, a transportation worker identification card, say, Monday: "Do I have handcuffs for four years out there? You can't say anything about TWIC?" I think not. But the chairman made a pledge, and so I'm going to stop here and ask the chairman to explain the pledge to the other members of this Committee.

MR. ROSENZWEIG: That's wonderful. I've actually already begun to redeem that pledge in the time since I made it. This is the second or third time the members of this Committee have expressed an interest to me in being able to break the bounds of the formal report mechanism and provide realtime input into ongoing developing projects within DHS, whether that be the Homeland Security Ops Center or TWIC or Secure Flight, being the three that come readily to mind.

We are bound in some ways by FACA -- Federal Advisory Committee Act -- laws. But my commitment, in speaking about it with our Federally Designated Officer, is that we're going to find a mechanism that is compliant with the law, obviously, but that will enable us to do some work on a closer-to-realtime basis with a public disclosure function thereafter. I'm hopeful that will happen by December.

MR. BARQUIN: Aside from RFID, what other technologies have you been at least talking about?

MR. PALMER: I'm glad you asked that. Secure Flight; TWIC card; behavioral pattern recognition; risk remediation priorities -- as a tool, not a process; and efficient document verification at checkpoints; access control devices; and, of course, the B-word: bomb. And, of course, there's also in the spreadsheet, Technology 1, Technology 2. TBD.

Not to mention goulannes (phonetic.) None of us can actually remember how to spell it; we just like to say it.

MR. BARQUIN: I thought it was big cows.

MR. ROSENZWEIG: When we've reached that levity point, it's time to move on to the next subcommittee.

Jim and Joanne, you have 15 minutes, and then I will redeem my promise to you to start with the next panel promptly on time. What is being presented now is a draft not for adoption for today but to begin with a discussion, both with the Committee and with the

next panel. And in the public, there's public commentary on a framework for analyzing privacy issues, which I will let either Jim or Joanne, the co-chairs -- Joanne McNabb, describe for the Committee their plans for its interim use.

MS. McNABB: Thank you. What we have in the book here is a Framework, as Paul just said, for analyzing the programs and technologies and applications that this Committee is going to consider. And I want to first briefly provide a little framework for the Framework and then let Jim describe the contents of the Framework.

This document, which is a draft and labeled as such, is intended to be used by the Committee as an, ideally, helpful tool, a list of questions to ask and approach for looking at and developing advice on the various programs that we'll be looking at. It's not intended to be a format for writing reports or a rigorous layout that must always be followed. And it's also intended to be helpful to the Department of Homeland Security as it develops its various programs.

And what we want you to do with it at this point, fellow Committee members, is take it back to your subcommittees and test-drive it; try it out on the various programs that you're working on between now and December, and then when we meet in December, we'd like to get your input, discuss it, get some discussions on how it might be improved and to find out how useful it possibly might be, and then potentially offer something for adoption then.

And now Jim will describe the contents of the frame.

MR. HARPER: Thank you, Joanne. The front page has a summary, which is probably better than I will be at laying out how the Framework works. I'll walk through it just quickly. I think I can be quick about what we hope to envision and what we will learn. I think we, frankly, will learn -- we've already learned -- and definitely benefit from the test-drive and the study that you all will give to the document.

Suggested Item 1 is to frame the scope of what you're studying. One of the things I guess we've learned is that that's not just a rogue exercise and it might take some effort to determine the scope of what the program technology or application is that you intend to study.

We anticipated, Joanne and I, that the DHS would provide us with scope, but we may have to determine scope ourselves and say that this is what we're talking about and that we're not talking about other things.

Legal basis is a step that should be perfunctory, essentially. Programs are there because of law, and I think it would help all of our audience in the public, press, and Congress to know what the legal framework is of the things that we're studying. Some of the inspiration for this comes from my experience in Congress, where, as a rule, you state what your legal authority is, what the constitution authority is for passing this on and so

forth. It will lend to the informativeness -- there's a better word than that -- of any document we put out to include legal basis.

Why don't I skip over Step 3 and come to the last, because it leads into the panel that we'll hear from next and gets to the real heart of what our result material is going to be, which is the effects on privacy interests.

We spent a lot of time and commentary -- not only from within our subcommittee but from without -- on this section, which is the heart of the privacy work we're doing, and we tried to establish a list of questions that go to the privacy interest that might be affected by the program application technology, and so on.

This is a new way of talking about these privacy interests, but it's also, I think, deeply rooted in orthodox privacy principles, if you will. Most of the principle statements we've seen to date are essentially -- I regard them as instructions to institutions; that is, "You should provide access," "You should do this," "You should do that." And those are good, the principles.

What we've done, essentially or theoretically at least, is turn those principles inside out so that they lead with the value that they represent. So we say "privacy," and then ask questions that go to that, subparts being: confidentiality, anonymity, freedom from surveillance, fairness, liberty, data security.

And I think by leading with those privacy values, we'll come up with results that are much more persuasive to our various audiences, that ordinary people can understand better for themselves; so rather than talking about institutional practices in a sort of abstract and, perhaps to real people, boring way, we'll be talking about values, stuff that they care about, stuff that real people worry about.

So we've already -- Joanne, in fact, has thought of ways to change these and do them better. We've gotten some comments. We certainly welcome comments from subcommittees or from individuals on how to improve this. It is a test-drive document, so take it home and study it.

Step 5 is the conclusion. I don't think we have to tell you, but what we propose for the conclusions is your conclusions: how things can be done better, whether our program should fly as-is, whether it should be stopped or delayed or whatever people feel is appropriate after they have gone through these steps.

Returning to Step 3, risk management efficacy. I think Joanne and I found, the more we thought about it, that in order to make some of these important determinations about the privacy consequences of things we're looking at, you have to understand what the benefit is you're going to get from a thing. You can't say that a thing is thumbs-up or thumbs-down on privacy without knowing what the end result is going to be.

And the best -- The best framework for thinking about that that we could come up with was the framework of risk management. And I'm not a risk management expert, though I have had a taste of it and I have certainly learned a lot since I started. Now I definitely know what I don't know about risk management.

I know a few things, though, and that is that we are all risk managers ourselves. An example being that we carefully weighed the benefits of coming to this room from the hotel over there, given the danger to ourselves of being hit by a car. I think we all made the right decision, but we did balance that risk.

Likewise, at lunch today, we balanced the risk of acquiring heart disease against the benefit of having another cookie or brownie. I chose twice, for heart disease. So we all make decisions like this all the time, and everybody does it. Like information, risk is all around you once you start to think about it. But I think we can all benefit from learning more about how risk management works in an articulated, more principled way.

And so for that reason, Joanne and I put together a panel of experts to discuss risk. So along with taking home the document to study, I hope we'll all carefully consider and listen to our risk management experts, who not only deal with risk management but also with risk communication, which I think is a unique problem in the terrorism area, because part of what terrorism is is scaring people, and what the public knows about things is an important aspect of what consequence terrorist acts might have.

So it's a fascinating area, and I think to the extent we can -- and, again, the Framework is not a blueprint -- but to the extent we can -- something about what risk management -- the DHS is doing with programs should be included in the material we put out.

So that concludes the summary of our document.

MR. ROSENZWEIG: Does anybody have questions for Jim or Joanne regarding the Framework? Joe.

MR. ALHADEFF: I just had a question on the concepts in the way risk management was being used, because I would think of it more as a two-step than a one-step process. And I think you-guys may have put it into one step, or I may just be misreading the summary of it; and that is, risk management deals with identifying the risks and ways to mitigate them in making determinations as to what may be acceptable risks that you're willing to live with.

There's another analysis that has to be made as to whether or not there's a benefit that taking those risks is worth or not. Where does the benefit portion of the evaluation come in? Is it part of the risk portion, or is it something that happens later?

MR. HARPER: What we're specifically focused on is the national security risk management piece of whatever you're examining. That reflects the benefit side of the cost/benefit equation you're doing in the totality of the document. If that gets to your question...

So the risk portion says, "Here's the benefit that we aim to get, as a society, from this program." The cost, privacy values are in the next step.

MS. McNABB: And, yeah, I think it's in the third step, in a sense. It's looking at, "Absent the privacy values first, here's the risk that the item, the program is intended to overcome," that being one sort of benefit. Then we go to the privacy cost. And then finally in the conclusion is where you do this (indicating) and make the recommendation.

MR. HARPER: Because the word "risk" has many different uses, we often talk about risks created by programs. And there are security risks, for example, with RFID, surveillance risks and stuff like that. And that's included as the last step in the risk management description, which dubs the response: "Does whatever program you're looking at create new risks to the asset or to others." So it's like an onion process, in that sometimes you create new risks by eliminating old ones.

MR. L. HOFFMAN: I'm assuming it is a draft, so I'm assuming you're open to fine-tuning the nomenclature. I thought this a long time ago, so I'm interested in hearing from the upcoming panel also how it's described these days. But in the old days, I remember breaking up risk into things like analysis management and communication and having a general area of risk and subdivide it and piece it together accordingly.

But I just want to note that for the record. It might be a minor change in nomenclature, but what we're getting at is the same thing.

MR. ROSENZWEIG: Ramon.

MR. BARQUIN: I really liked, in general, the approach. I just have one question/comment; and that is, in the glossary at the end, aside from the privacy definition, which is dually attributed to Alan Westin, of course, I don't -- I just want to make sure that as we move ahead -- and this can be extremely useful and helpful, but given that we're going to be dealing a lot with most of these terms, I think it becomes important that we all agree with the definitions as expressed in this Framework paper and, wherever possible, that we can be consistent in the future with our terminology.

MR. ROSENZWEIG: In fact, if I recall at our very first meeting -- I think it was Jim Sheehan, who's not here today, who said that one of the first problems that we have was defining the shape of the table.

So I think that this is useful in helping us define the table. I should add, it's implicit in the fact that we're having this discussion here in public and have distributed this, but

this will be on the website, and some of our public commentators may want to, besides giving us lessons on risk in the upcoming panel, perhaps provide us with their feedback directly on this document.

So there's an open invitation to anybody out there.

Tara.

MS. LEMMEY: I do encourage everyone to engage in this dialogue, because I think it's an interesting process, at least the parts of the Committee that I've been able to make in having this conversation, because value is rarely talked about in the privacy conversation. And so it's really worth getting a lot of input on the value statements, just to see if we agree on those.

Just reading it again now -- I've already read it six times already -- I realize how the liberty agreements would have a chilling effect on speech, because we frequently don't think about privacy and speech tied together, yet they're tied tightly together. And on the risk components, Markle Taskforce is going to be issuing a new report in December with a huge section on risk. And there's some background that I can probably share to your point, Joe, about the component parts on both sides.

There's some very good research that was done by the DoD on, well, both the risk of doing stuff and the risk of not doing stuff and where we're making tradeoffs. We used to be making tradeoffs very much from the need to do it at the last possible moment, and you can't do that anymore.

You have to shift that risk profile, and it's a tough proposition because it changes the whole balance. So for any of you who want to dig deeper on risk, I'm happy to share some background.

MR. ROSENZWEIG: I'm sure that our co-chairs wish to dig deeper. They set up a whole panel for that purpose. And unless someone feels a burning need to continue this discussion, to that panel we will now turn. I would ask the panelists to come up and join us.

First, a couple of notes. Rebecca Richards, our Designated Federal Officer, tells me that we have nobody signed up for the public comment period, from 4:30 to 5:00. It's three minutes a person. If you want to speak to us, please see her during this time and put your name on this list.

MR. HARPER: Can they use pseudonyms, so if people wish to sign up without identifying themselves?

MR. ROSENZWEIG: No. If they want to talk to us, they've got to tell us who it is.

This panel has considerably introduced us to purpose already. I'll let Lisa tell you who's on it.

MS. SOTTO: Thank you, Mr. Chairman. We have a wonderful panel coming up that I'm very anxious to hear. Starting with Professor John Mueller. Professor Mueller holds Woody Hayes chair of National Securities Studies at the –

COMMITTEE MEMBER: Woody?

PROFESSOR MUELLER: Woody. Absolutely true.

MS. SOTTO: And Professor Mueller is also a professor of political science at Ohio State University, where he teaches courses in international relations. He is currently working on terrorism issues and, particularly, is focused on the reactions to or overreaction that terrorism often inspires.

And I want to note also that Professor Mueller is the most well-rounded person in the room. He has written a book called Astaire Dancing, which has won a prize, and also has written two scripts for musicals. Congratulations.

PROFESSOR MUELLER: Thank you.

MS. SOTTO: Professor Paul Slovic also joins us. Professor Slovic is the president of Decision Research and a professor of psychology at the University of Oregon. He's the past president of the Society for Risk Analysis and received in 1991 a distinguished contribution award. Professor Slovic also received the distinguished Scientific Contribution Award from the American Psychological Association and the Outstanding Contribution to Science Award from the Oregon Academy of Science in 1995. Thank you for joining us.

And, finally, Detlof von Winterfeldt. Professor von Winterfeldt is a professor of public policy and management at the School of Policy, Planning, and Development at the University of Southern California and is also the director of the school's Institute For Civic Enterprise. His research interests are in the foundation and practice of decision and risk analysis and applied technology and environmental problems, and he served on several committees of the National Science Foundation and National Research Council.

Welcome to all of you.

MR. ROSENZWEIG: Gentlemen, since the purpose here is educational for us in an area that is perhaps a little outside for most of us, we'll extend some time and hope that you'll use that to educate us. If you'll keep your talks to about 15 minutes, we have about an hour and a half to have this discussion, and that will be plenty of time for our ignorant questions that reflect our lack of information. But if you'll go in the order you were introduced...

PROFESSOR MUELLER: Thank you. Very nice to be here. This is the first time I've ever talked before any group dealing with Homeland Security, and this may also be the last time I ever do so.

What I'd like to do is look extremely broadly at an international relations perspective, while leaving the risk analysis to Paul Slovic -- I'm not quite suicidal enough to engage in it myself with him sitting next to me -- and suggest that quite possibly the whole threat has been massively exaggerated and the reaction to it has been more costly than the threat itself, even the potential threat, in many respects.

I am currently working on a book, sort of comparing threat exaggeration or threat assessment over the last 50 years or so, and it's tentatively entitled Devils and Duct Tape: Terrorism and the Dynamics of Threat Exaggeration.

What I'd like to sort of start out with is a quotation from Michael Moore, everybody's favorite provocateur, who said on 60 Minutes a couple years ago that the chance of any of us dying by a terrorist attack is very, very small. And then his interlocutor, Bob Simon, said, "But no one in the world believes that." Both statements are true, and it strikes me as being a really monumental absurdity.

It seems to me that, basically, if you step back from the terrorism situation, international terrorism actually does very little damage. The number of people killed each year by international terrorists before 9/11 and since 9/11 has been basically a few hundred a year, not many more than are dying drowning in bathtubs in the United States. The number of Americans who died, outside of 9/11, of course, from international terrorism is smaller than the number who have died from lightning. The number of Americans in America who have died from international terrorism, outside of 9/11, is smaller than the number who have died from drowning in toilets.

It's not necessarily a monumental situation, it seems to me. It's something that's fairly incidental in a lot of respects, and perhaps I'm suggesting we should at least spend some time thinking about it in, perhaps, those terms.

The argument, of course, is that 9/11 was a harbinger, rather than an aberration, and my suggestion is that maybe it is simply an aberration. There's a lot of concerns that everything I've said is true; however, what's going to happen in the next 20 minutes is that Osama bin Laden is going to figure out how to do -- nuclear weapons or chemical weapons or biological weapons, and I think those are fairly unlikely. Extremely unlikely. In general, it seems to me that the most likely situation is that there will be some sort of terrorist attack eventually, but its ramifications and its effects will be really quite limited and really quite absorbable, maybe grimly but nonetheless.

And so, consequently, instead of spending a huge amount of money trying to prevent something which is essentially unpreventable, it would be better simply to save

the money and then spend it trying to fix the damage when it actually happens, then go after the perpetrators, assuming they're still alive. There's a tiny probability that it will be a catastrophic event, but it seems to me that that is so small, that it can mostly be discounted. And I will be glad to go into that more if you want.

Chemical weapons, for example, are an incredibly inefficient way of killing people. In World War I, they had gone up for 7/10ths of one percent of the battle. Biological weapons still haven't been developed effectively, even though nation states have been working on them for eight years, and even at that, the biology hasn't been developed a whole lot. Nuclear weapons are extraordinarily difficult to put together. It's taken Iran ten years to develop a nuclear weapon, and that's a state, not a small terrorist band hiding out, sharing a tent with a well-hung Koran in Afghanistan.

Anyway, it seems to me that what's likely to happen is not terribly monumental. And my big concern is that the reaction to terrorism generally seems to be worse and more costly than terrorism itself. That's even the case with respect to 9/11, which is by far -- by far -- the biggest terrorist attack in history, most costly in history. In terms of economics, for example, when it's calculated that -- and this is highly relevant, it seems to me, from some of the discussion earlier today -- is that if you increase the waiting time by half an hour for all passengers in planes, that costs the economy $15 billion every year. It seems to me -- and this is probably exaggerated, that when airlines make a profit, it's usually about $5 or $6 billion dollars per year. Now they're losing that much. But the point is, it should be part of the consideration as well. Incredible economic cost that attend to many of the ventures that try to deal with that.

Similarly, there is a situation with respect to the human cost. A study has come out at the University of Michigan, trying to calculate how many people were killed in automobiles between September 11th, 2001 and the end of the year, because they drove rather than flew, and the answer comes out to be more than a thousand.

In addition, of course, 9/11 facilitated two wars, Afghanistan and Iraq, which have now killed at least 3,000 Americans: civilians and military. If indeed 100,000 Iraqis have died because of that war that will represent more people that have died at the hands of all international terrorists in all of history. What I'm trying to argue for is sort of putting this in that sort of context and dealing with the issue of overreaction and overfear and argue that what really seems to be the problem is not so much what the terrorists do, though obviously one must pay a fair amount of attention to that, but the reaction to it and the cost of the reaction.

I've just recently been given an extremely good example of this in many respects by the U.N. report of about two weeks, about what happened with Chernobyl. An extensive study indicates Chernobyl is the worst nuclear disaster in history. It's very hard to

imagine one that could be worse, by a terrorist or anybody else. It, of course, was not due to terrorists, but nonetheless...

That total of human cost of that is about 50 people. 47 people. That's how many people have died because of the effects of that. There's some possibility, which is not at all certain, that as many as 4,000 people will come down with cancer in due course, though they haven't done it yet, died of cancer.

But this report also says that by far -- by far -- the biggest physical health effects of Chernobyl was the fear of Chernobyl. Women as far away as Italy were aborting babies because they thought they would be born with three heads. The huge amount of alcoholism, discontent, fatalism, dejection that has come out of that, according to this report, have been much worse; the health effects of that have been much worse than the actual event itself. And it seems to me this is something that ought to be really taken into consideration in a major way.

In terms of terrorism threat within the United States, we have to, I think, sometimes think about the fact that there haven't been any. I'd like to -- And we keep getting these reports suggesting that terrorists are, perhaps, everywhere. Let me give you a comparison of Robert Mueller, head of the FBI, he has now adopted the policy, "I think, therefore they are." In early 2003, he said, "We haven't found any terrorists yet, but what I'm really worried about are the things we can't see." And he said at that time, early 2003, "The terrorists are in this country," though he hadn't seen them, hadn't found them. "They have the capacity to do huge damage, and they want to do it." Okay. It's now been two years since that time, 2005. In the meantime, the United States launched what might be considered to be a major provocation to the terrorists -- namely, the invasion of Iraq -- and it still hasn't happened. And earlier this year, testifying before the same Committee, Robert Mueller said, "What we really have to worry about are the things we can't see." And then it's underlined in bold on the FBI website a report of what he said.

At the same time, however, the FBI had produced a secret report -- why exactly it's secret is beyond me -- which was leaked to ABC News -- fortunate for me -- which suggests that after four years of huge amounts of efforts, huge amounts of expenditures, the FBI is yet to be able to identify a single true terrorist cell within the United States.

There's three possibilities, I suppose. One could be that the FBI is incompetent. The second is that the terrorists are incredibly clever. And the third is that they don't exist. I don't know which of those is right, or maybe it's a combination. But at any rate, at the same time he's specifying "What I'm worried about are the things you can't see," there was a report on his desk, which is still apparently secret, suggesting that they basically were not able to find anything.

If I can make two comparisons, which sort of come out of my longer range perspective: During World War II, there was a great fear that the Japanese citizens in the United States were going to be committing espionage and sabotage; so, therefore, hundreds of thousands of them were locked up over the course of the war. It's also the case that, zero, none of those people have ever been found to have been guilty of anything. There's never been an indictment of any single Japanese-American citizen, or even a Japanese-Japanese citizen, for that matter, within the United States to commit such. Zero.

Short after World War II, there was grave concern, in the McCarthy era, about domestic communists, the enemy so vast, the vast conspiracy. After World War II -- And at no time, as far as they know, did any member of the Communist Party commit an act of sabotage, which is sort of like terrorism, and what they were primarily concerned about were defense plans. In addition, after World War II, as far as they know, the Communist Party never committed any act of espionage within the United States.

In both cases, they report an internal enemy and capacity of the internal enemy. In the case of the Japanese, it wasn't an enemy. In the case of the communists, it was an enemy, but it seemed to be incapable of doing very much. In both cases, they were vastly exaggerated.

Now, it doesn't follow, therefore, that terrorists are not important and can't do bad things, but it does suggest that possibly we've exaggerated the threat. Okay. Let me just make a couple of final points here. I'd planned to speak only five minutes, so I'm probably not going to get up to your 15 minutes.

MR. ROSENZWEIG: For which we will thank you.

PROFESSOR MUELLER: Okay. Thank you. It seems to me in some of the discussions that we're dealing with today that a huge amount of money is being spent to protect the United States against something that is impossible; namely, the idea that someone can hijack an airplane, take it over, and fly it into a target. That may be a lack of imagination, but it is essentially impossible.

The reason it worked in 9/11 is because previously the idea was, if someone hijacks an airliner, you try to reason with them and get them on the ground and negotiate with them. And 9/11 obviously changed that and we know that from the fourth plane, because even though the passengers on that plane only had fragmentary evidence about what was happening to the first three planes, they nonetheless adopted a new policy subsequently, which was to overcome the hijackers. They were not able, obviously, to save the plane, but it never crashed into the target that it was intended to go for. It seems to me that was very likely.

Now, some people argued, "Well, they could possibly still do that. You know, maybe get somebody in with a Latin-American accent and calm the passengers by saying, 'We're just going to Cuba.'" Bruce Schneier basically suggests that, "Well, maybe if they're carrying a baby they could get away with it." It just seems to me that it's extremely unlikely that that would happen. And maybe I'm wrong, but it seems to me that should be a core part of the discussion. And therefore, the portion of the Homeland Security budget that is going to prevent that calamity might be massively misappropriated. It may be just a terribly foolish expenditure over all.

Finally, I'll talk about what I call the terrorism industry. The huge amount -- If fear is the big problem, it seems to me that what should be done is some effort to reduce the fear -- and Professor Slovic can certainly talk much better about this than I -- I'm pretty pessimistic about that possibility. But instead of efforts to try to reduce the fear and, sometimes, even hysteria, and very occasionally even panic over this issue, most of the terrorism industry, as I call it, is devoted to exacerbating the situation. The politicians of both parties seem never to talk about -- I mean, basically nobody ever says what Michael Moore said. I have been looking very hard to find people who have said it in print or in television, and I've not found anything. I mean, hardly anybody ever says that the chance of an American being killed by a terrorist is very, very, very small. It seems to me the Department of Homeland Security should be saying that or else give us evidence that it's not true. Anyway, it should be discussed, and it's not there.

Almost no one ever says what I just said. I've looked very hard to find places where people said that it's impossible. I found a guy named Banks who did and one other book, saying that it's impossible that a plane could be hijacked and used to crash into a target. It seems to me that should be part of the dialogue and there should be efforts at least to try to calm the fears, even though that might not be terribly effective.

On the other hand, what you get is what I consider almost the hysterical material: people talking about apocalypse, people talking about that the state system can be destroyed by terrorists with bombs. There's an existential threat to the United States.

And let me just conclude with one quotation from General Myers, the chairman of the Joint Chiefs of Staff. He was on television about a year and a half ago. And he said that "Well, what the terrorists really want to do is to do away with our way of life. They couldn't do that when they killed 3,000 people on 9/11, but if they could kill 10,000, that would do it." And nobody said, "General, would you please explain how our way of life goes away if 10,000 people die." We have this football stadium in Columbus, which should be named after Woody Hayes but isn't, and it seats 100,000 people. I've been in it when it's full, and I can sort of understand numbers like 100,000, sort of, and I can imagine what it looks like when it's only one-tenth full. That would be pretty empty, but

if those people were suddenly killed by terrorist, that would be a horrible tragedy, the worst to have ever hit the United States since the Civil War.

Also, by the way, 10,000 was the number of people they thought might have died in New Orleans, right? And that would have been horrible obviously, and the number might indeed grow upwards somewhat, but no one seemed to think, "Okay, that's where we have to stop existing." But the basic idea is that somehow that would destroy the United States, it would strip away our way of life. It seems to me the only way that can happen is if we do that to ourselves. You know, we'll have to stop eating hamburgers, close down churches and the First Amendment, start learning Korean, and eventually it would somehow do away with our way of life. That is to say, what these people seem to be suggesting is that it's not the terrorists who are suicidal, but, rather, we are.

And talk like that to me seems to exacerbate the major problems of terrorism, which I think is this type of overreaction and this sense of hysteria. It happens with politicians. It happens with bureaucrats. It happens with the media; it always leaks, of course. And it happens with, you know, pundits and so forth on television. And it's very, very rarely refuted.

It seems to me this whole -- I guess what I'm trying to say, finally, is -- to end this, is that the perspective I'm putting forward, what I'd like to persuade you of is a reasonable one. I mean, you may disagree. Plenty of people have disagreed with me at various times. But it seem to be reasonable, and it should be part of the debate. You may say, "Okay. I heard you, and I still think you're wrong. The terror is really there, and there really is a danger and these guys might" -- Okay. That's, you know, fair enough.

But what bothers me not so much that I may be wrong but that this perspective, which I think is a reasonable one, is not really in public debate at all. It should be there, and it simply isn't.

Thank you.

MR. ROSENZWEIG: Thank you very much. Professor Slovic.

PROFESSOR SLOVIC: Thank you. The topic of risk is an extremely complex one. Some of us have been going decades to try and understand it. I'll give you a quick overview in ten, 15 minutes, but obviously it will be rather superficial. I hope it will be useful nonetheless.

Human beings have been dealing with risks, obviously, for hundreds of thousands of years, if not longer, and there really are two ways in which we today deal with risk. One is through analysis, but the more basic way is what we call risk as feelings, and that was the mode that helped us survive the course of human evolution over all those years. We didn't have quantitative risk assessment to try to guide us. We used our instincts and our gut feelings to decide whether this animal lurking in the shadows was safe to

approach or whether the funny smelling water in the stream was safe to drink. We used our senses.

Today -- Well, over the more recent evolutionary time, we have come up with other ways of dealing with risk, because it wasn't good enough to just rely on risk as feelings, so we've developed many different sciences and analytic methods to help us surpass our intuitive capabilities.

So today, you know, we walk around; our brains are kind of wired to think in both ways. And psychologists call this dual process Theories of Thinking. And dual processes are experiential or -- you know, intuitive versus analytical.

These two systems of thought reside in us sort of side by side, and they're constantly at play and interacting with each other in what we call "the dance of affect and reason." There's a lot of research going on right now to try to understand the nature of this dance. We understand it somewhat but not fully adequately. And I'll try to describe that very, very briefly.

But in any event, the technical analysis of risk: Risk assessment relies on data and evidence and statistics and is fairly sophisticated, and it needs to -- I see risk communications as part of risk assessment. And kind of in between this path of risk assessment and risk management are some messy things that deal with risk perception and this more intuitive mechanism.

And what we find is that, you know, risk is really incredibly complex. So if you're going to enter into risk as part of your Framework, and that's the Framework doctrine, I think it would be helpful to appreciate what you're getting into.

So first of all, just the very definition of the term risk, as Jim alluded to a few minutes ago, is not obvious. We use the word risk in at least four different ways. We use it to designate a hazard, something that is hazardous; like, flying in an airplane is a risk. We use it when we really mean probability. What is the risk of getting AIDS from an infected needle? It's sort of implying "What is the chance," "What is the probability?" We use it when we really mean consequence. "What's the risk of letting your parking meter expire?" It's getting a ticket. That's the consequence. I think the most legitimate use of the term is some combination of likelihood and severity of consequence, for which we might just designate as "threat." So you can see, by the way, that the language of risk is sloppy, and that's just the beginnings of the problem.

Another thing that one has to be aware of is that risk is inherently subjective, when often -- Here is the term, "objective risk." Well, I don't think that is a correct term. I think that risk is a construction of the human mind to help us think about the dangers in the world. And the dangers are real. Clearly there are things in the world that can harm us.

And we have then created a term called risk to help us -- supposedly help us think about and manage and deal with these dangers.

But when you start to look very closely at how we measure risk, you see that you have to -- it is rife with assumptions. So if you're a toxicologist and you want to assess the risk of a small exposure to some carcinogenic chemical, you may give this to animals. You may dose animals at very high doses for a couple of years and see what kind of tumors arise. But then you have to extrapolate to humans, who are exposed to very different conditions, and you use mathematical models and a lot of assumptions. So it's rife with assumptions Even the most simple types of measures of risk, say, that are based on counting fatalities, and what could be simpler than counting deaths and then dividing them by the number of people exposed to something to get some rate? That's really simple.

But if you do that, you're giving equal weight to every manner of death. Do you say whether this person was young or old? Do you say whether the exposure that led to death was voluntary or involuntary? It doesn't matter. Or whether they were getting a benefit from the activity? Whether or not, it doesn't matter.

So there's a value judgment there, even at the simplest level. So risk assessment is inherently evaluating. And if you're going to start to assess risks in the security or privacy domain, then you're going to have to ultimately think about, well, what are the consequences that you're protecting against and how are they valued. There was a brief discussion of this in the last hour, of which child do you want to sacrifice or whatever. I mean, there are tough value issues in dealing with the consequences in trying to come up with a measure of risk.

Finally, risk is not necessarily the best way to make decisions about hazards because it focuses you on one side of things. Obviously, if you're going to make -- For decision-making you need a broader perspective that takes into account, you know, what are the alternatives -- that was mentioned earlier this afternoon -- What are the alternatives? What are the benefits, you know, weighed against the risk? So you need a broader decision framework, and I assume Detlof, who's a specialist in decision analysis, will get into this in a minute.

Once you get into perception, again, there's a lot of strange things that happen. And I agree with Professor Mueller about the reactions that we make are not always, perhaps, optimal, but you find it goes all directions.

So, for example, we find that expert views and public views are often different. And often it's the public that's derided. But if you look carefully, there's often a wisdom or a logic to public response, and where whereas the experts tend to focus on these probabilities and varying consequences in defining risk, the public has a broader set of

considerations that they take into account. They care about whether exposure is voluntary, whether the individual has control over the risk, whether there's the possibility of catastrophic accidents, whether there's a dread quality to the risk.

I mean, we are more concerned about things that cause cancer than things that -- than accidental deaths, even though you're equally dead either way, but cancer is a dread disease. This issue of dread is very relevant to terrorism because the nature of terrorist acts evoke dread in us; they are dreadful consequences. The notion that another person is out to harm us in this way, even by killing themselves for the motive just to creator terror and destruction is very difficult for us to think about and tolerate. It's a very distasteful type of hazard, and so we react more strongly. It's intuitive. We call it affect. This affect of response is very powerful when you think about terrorism.

We also, in the modern study of affect and reason, we see the importance of imagery. And not just visual images. Images are words or sounds or sensations that come to us. And the research has shown that if an outcome is highly affective, there's a lot of emotion to it, then we disregard its likelihood. This is very relevant to what Professor Mueller was just describing.

So if the outcome is dreadful, then we have this strong negative feeling, and it makes us -- it confuses us about the false-positive likelihood. We treat it as though it was likely. Why? Because we feel it so strongly, it must be likely. We confuse "likely" to probability and consequence. It causes something that is now known as "probability neglect," and I think that this is what the first speaker was alluding to, that we are treating things that are remotely likely in a way that -- We're kind of giving them a respect that they would be accorded if they were more likely.

Anyway, we have to be aware of it because -- Ideally, we need both types of thinking. We need the analytic thinking, and we need the affective thinking, but we should do the analytic thinking to kind -- as a check on our affective response. I'm not saying our affect or our experience of responses are irrational. They're not. That's a very sophisticated system, this intuitive system. It's like perception, very sophisticated. But they do go wrong, and we need to have both systems kind of putting a check on each other.

We're starting to do risk perception studies on various types of terrorist attacks, versus accidents and diseases and other things that can take lives. And we're finding, not surprisingly, that the perception and response to a terrorist act is much stronger than another type of event that causes as much physical harm. That's not surprising.

What is interesting is that the response, as far as we can determine, is very insensitive to the number of lives lost. So if we give people scenarios and we vary the life loss from zero to 15, to 495, we find that that's not relevant. The response to a terrorist act,

the response is as strong for zero or 15 lives lost as it is to 500. That's just another element of the affective response.

Finally, on the communication side -- it was brought up -- You know, terrorism is about fear, and how do we communicate in ways that put this in perspective? And first I would say that communication attempts need to be developed through research and study just like other aspects of this assessment. You need to test your messages. You need to try to understand what's going on in a perceptual manner in order to craft your messages.

So, for example, we know that risk perception, one of the key elements is control, so if when one is communicating, I think it's important to communicate to people if there's some threat. Well, what are the avenues of control out there? What is the government doing? What are other officials doing, health officials and so on, to control this risk? What avenues do you have as an individual to control things? Because if you see the threat as uncontrollable, then that's when there's a dysfunctional response.

So in that way, I think that you need to kind of collaborate with the people you're communicating to, to understand their concerns and to work with them to develop messages and then test those messages to see whether they're effective. And that's a research enterprise.

And I think I won't take my last 30 seconds.

MR. ROSENZWEIG: Thank you very much. And Mr. -- I'm not even going to try. Tell us what it is.

MR. VON WINTERFELDT: It's von Winterfeldt (pronouncing). And the German is von Winterfeldt (pronouncing). It's a pleasure to be here and to be a part of the thoughts on risk analysis and risk management and privacy. I graduated a little bit -- I'm not anymore the director of the Institute for Civic Enterprise. I'm now the director of the Center For Risk-Based and Economic Analysis of Terrorism at the University of Southern California.

What I'm going to do in the next ten minutes or so is to talk a little bit about what our Center does, put that in perspective. To tell you something about where we are with risk assessment and risk management in the terrorism arena is absolutely one of our major challenges, and to the extent I could stress my imagination, speculate a little bit about the privacy issues in all of this, maybe that could be helpful.

So the Center for Risk and Economic Analysis of Terrorism -- and if you look at the first letters, it spells CREATE. So CREATE was the first university-based Center of Excellence funded by the Department of Homeland Security at about $4 million a year for, initially, three years. We're on our second year right now.

We have three other centers in existence that you may know of. Two are concerned with food and agricultural terrorist events and one is concerned with behavioral and social events; behavior of the terrorists on one hand and behavior of the public in response to terrorism on the other.

All of our focus is on risk analysis, risk assessment, increasingly on risk management -- we're still slipping into that -- and on economics. There's a front end of the problem and a tail end of the problem. So we're looking at the threat of vulnerability; the events that could occur, the probabilities of that; and when they occur, we analyze it and look at the economic importance.

Economics are very important, just as Professor Mueller mentioned, because small events can have huge economic impacts. For example, a bomb attack on the Los Angeles harbor could shut the harbor down for several months at a cost of about $20 billion a month.

Okay. Let me briefly talk about terrorism versus assessment and risk management. I'm using the terms risk analysis and risk assessment interchangeably. I think that's fairly common, standard, in our field.

Risk assessment and risk analysis is a discipline in nonterrorist areas. It's got a history of more than 30 years. It originated with reliability studies in the aerospace industry and then in the nuclear power plant industry. There was a pivotal study in 1975 by Rasmussen that developed most of the contents of risk assessment that we now use today.

Expanded from there to other engineering fields, chemical plants, etcetera, environmental areas, EPS was very instrumental in natural disasters. In trying to know the history of that, there's a very important event, which is a publication called Risk Assessment of the Federal Government by the National Academy of Scientists in 1982 which laid out many of the principles that are still governing our work today.

What's different about terrorism is -- Well, let's put it this way: Some people just thought we could just use the tools and apply them to terrorists and then we're done with it. I don't really use that. There are a lot of differences in terrorism.

First of all, terrorists don't act like nature does. An earthquake doesn't choose the time when it wants to go off. In other words, it doesn't mind -- it doesn't select the time when everybody's out on the street. Terrorists would look at situations where we're weak and when they can inflict the worst damage. That's one difference. The other difference is that once we plug one hole against terrorism, there is what we call risk transference. The risk will shift to another area.

We currently structure terrorist risk assessment in three steps. Threat analysis, dealing with developing attack scenarios, and attaching probabilities to that method.

That's a very, very difficult task, and I don't think we have any -- We're making small steps and we're having some successes in that area.

And the second step is a little bit better understood, and that's vulnerability analysis, where we're trying to assess the probability of success of an attack, success from the terrorists' perspective if they attack.

And then finally, the best part, the part that's best understood, is consequence analysis. So if you have an event, you can pretty much predict what the vast effects are, even what the biomedical epidemiologies that are going to apply, and those things are pretty much off the shelf. But it's the threat analysis that's very difficult. Now, briefly on risk management, once you have analyzed the risk and said, "Okay, if we don't do anything, here's what it looks like," then you have to start thinking about alternatives to deal with it. You can decide not to do anything. Maybe probability is low enough. Consequence is low enough.

But in some cases, for example, with a nuclear device, probability is there. It may be very small, but the consequences are horrendous. And I don't quite agree -- well, I don't quite agree at all with Professor Mueller that one shouldn't be worried about that. I'm very worried about the nuclear device, and I'm very worried about the biological effects and many other things. So you have to think about alternatives, programs, technologies. And what do they do? You have to look at their ability to reduce probabilities and/or consequences. Some do both. Some do only probabilities, like deterrence activities or detention activities. We use probabilities and emergency response activities.

Then you have to assess the benefits of these alternatives, benefits in terms of the risk reduction and the cost. And in that first step I'm talking about real dollars. If you look at MANPADS, for example, MANPADS is one of the many, many risks against aircraft. The government is just about to think about spending tens of billions of dollars on countermeasures against surface-to-air missiles, MANPADS. For one risk, and whether that's a reasonable investment is a big question mark. But those decisions are on the table.

And then once you do it in the first rung, you do it in another rung, and that rung has to do with unintended indirect effects of the technologies of programs. And I think that's one of your primary concerns. One of the unintended and indirect is the privacy impact, is the impact on liberties and freedom, etcetera, and they have to be taken very seriously. But there are other impacts too: business impacts, inconveniences, fears. Then you have to evaluate and you have to implement the alternative and you have to monitor the implementation. So that's the whole package of risk management. I also see this as an interwoven activity.

Throughout the process of risk assessment to risk management, it isn't something special. All right. You have to do it early on. Privacy obviously comes in the middle of the risk management and risk evaluation aspect. These assessments of privacy won't necessarily be qualitative, not unlike equity considerations in cost benefit analyses.

But I think one can also do something quantitative in the privacy area. In particular, if you're interested in some methodologies here, there is a field called Signal Detection Theory. It's a very well-established, formal theory that looks at issues like false-positives, false alarms, and so on, the cost benefits and their probabilities. That is a tool itself that one can use to shake out the efficacy of the alternatives in terms of privacy and other indirect impacts. So let me end with a little think-piece on what one might call privacy risk assessment. I think you have a document here, Privacy Effect Assessment. I thought that was very interesting.

It's not unlike activities, like Environmental Justice Impact Assessment. I mean, you're looking at all these other things that occur when you take government or private action. The point that I would make is that this would not be an afterthought. These indirect effects, whether they're privacy or economic impacts or inconveniences, ought to come in early and be shaken out early at the stage when the options are still on the table.

Now, often the options are narrowed down by the time they come to you or committees like yours, and we say, "Well, here is what we want to do: Shake it out. See if we can make it a privacy issue somehow." If you back off of that and you look at the broader range of options, including doing nothing and including doing a technology versus a problematic option, I think you're much better off.

And then, of course, there are mitigation alternatives. In terms of mitigation, I'm not a privacy expert. But it seems to me a lot of focus on mitigation is on restricting access to information. I think it is equally valuable to look at restrictions on use of information and its access. And I know all the technologies to private information these days, I believe it's very hard to control information anymore in this day and age. But maybe it's possible to control user information once it's in the hands of appropriate people.

And the other one, I'm glad it was mentioned in this forum, is the redress or restitution issue. To me that's very interesting, because I would give out a fair amount of privacy issues and freedom if I knew that the government screwed up, at the end of the day I'd get a million bucks, or something of that nature. The problem with that, of course, is that the government doesn't like to admit that it made a mistake and the legal ramifications of that.

But if you could cut through that -- If you could use that poor guy up there -- where was it -- Seattle? The guy was mismatched for the Madrid bomber. I don't know

what he got out of it. He should have gotten a really nice, hefty sum. He's probably in litigation right now with somebody, right? I don't know what happened to that.

So those are my thoughts. The one thing that -- There's a lot of history in risk analysis. You don't have to reinvent that. It's useful. I thought your write-up was very thoughtful, very good. But looking at some of these documents might help you.

And also, another history, for some reason I saw an analogy to environmental justice history. So you might want to look at their trials and tribulations. And they're basically in the process -- The EIS process in general. Environmental justice aspect of the environment impact statement is really an afterthought to decisions that are frequently already made, and I don't think that's a good thing. I would hate to see privacy issues and unintended effects an afterthought of the decisions that are made somewhere on the 6th floor in Washington at DHS.

Thank you. And by the way, I have to apologize; I have to leave at 4:30 sharp, okay?

MR. ROSENZWEIG: We promise that we will conclude this panel at 4:30 or earlier. I want to thank you all for a very interesting set of presentations. I see a couple of tent cards. I do want to start with one of my own, and this is either for Professor Slovic or Professor Mueller.

Both of you, accurately I think, described how our assessments of risk are not often what would appear to be rational but are the product of emotion or -- I love the word "dread." But that suggests to me that what you are describing and what you're decrying, Professor Mueller, and what you're describing, Professor Slovic, is hard-wired, that it comes very much from -- I don't know: Genetic development? Evolution over the course of the years? There's a value to dread, I assume. Of course, it is unreasonable, by its very nature. And, at least in my own experience, reason cannot convince unreasoning conclusions. My mother won't fly. Period. Full stop. End of story. I can talk to her for forever about how it's safer than driving. She won't do it. And nothing will ever -- So assuming that your diagnosis is accurate, what is your prescription? How -- I mean, can it be fixed? What's the prescription?

PROFESSOR MUELLER: I'm very pessimistic about that. I think people should be trying, but I'm not very convinced it's going to be possible. Professor Slovic has done a lot with risk engagement, much more than I. But the issue, in many respects, is what should the government do because people are afraid? It doesn't follow that because people are afraid, billions of dollars have to be wasted.

People were shocked when the airplane was shot down over Lockerbie in 1988, including a couple of students at the university I was at at the time, and there was outrage expressed and so forth, and what the Bush and Reagan Administration did was, simply,

police work. They tried to find the people who did it eventually, and only because of incredible luck were they able to do so.

Even though there was a lot of outrage, they didn't have to spend a lot of money throwing bombs someplace or another. Previously, of course, Reagan bombed Tripoli because of the bombing in Berlin, which killed one person, and the Lockerbie bombing was a reaction by Libyan agents to that. Very counterproductive. So it doesn't follow that you have to do stuff.

Even 9/11 and Pearl Harbor conceivably would fit in that category, although those are extreme cases. When the Cole was bombed, nothing happened. The Anthrax Bomber, what's happened is there was a huge amount of money wasted in trying to protect the Post Office from anthrax and so forth. There certainly was a great deal of concern about it and people were very unsettled about it, but the government did not have to spend huge amounts of money on it necessarily. A certain amount of smoke and mirrors is probably important instead of saying "We're very concerned about this" and everything, but even extremists can be rather overcome. The experience is definitely there.

Furthermore, hyperreaction tends to be counterproductive often. When the bombs took place in Africa, Bill Clinton retaliated by bombing the pharmaceutical plant in Sudan, which probably resulted in the death of tens of thousands of Sudanese. They also bombed Afghanistan at the exact time that the government was negotiating turning Osama bin Laden over to the Saudis to be tried in Saudi Arabia. When the bombing took place, all those negotiations were totally broken off and Osama bin Laden and Omar leapt into each other's arms and cuddled into the protection of the Taliban.

So frequently these reactions that sort of seem good and feel good from a political standpoint are extraordinarily unwise. And you can somewhat finesse them. When terrorists killed a bunch of Marines in Lebanon in 1983, Reagan's reaction was to huff and puff and actually pull the rest of the Marines out. And most of the Americans said, "Well, I'm glad." So it doesn't follow -- People will still be afraid.

I'll just quote a few things. From Paul Slovic, actually. If I missummarize his research... He can correct me, but... "People tend to overestimate the chances of dramatic or sensational causes of death." "Realistically informing people of risk sometimes makes them only more frightened." I know airlines tell you how safe it is to fly. The reason is that if you tell them how unsafe it is to fly, they'll become more afraid to fly.

The strong beliefs in this area are very hard to modify, like your mother's flying ideas, than any new sort of calamity tends to be taken on future mishaps. Disaster tips increase fears, not only about that kind of danger but of all kinds, and that people, even professionals, risks are expressed. Far more likely, for example, to choose radiation

therapy if total chances of death are 32 percent, rather than the chance of survival, which are 68 percent: The source can also make a lot of difference.

PROFESSOR SLOVIC: Good quotes. A couple of comments. This question of rationality and our emotions being irrational. The problem is, it's not as simple as that. The emotional or affective system is extremely sophisticated. Just like perception. I mean, catching a ball; you try to model that mathematically, and it's very difficult. So it's a good system, but sometimes it can get us into big trouble. It can lead us -- it can be a mistake.

But so can analysis. You know, it can get us to the moon; it can create machines that fly; it can do a lot of things. But it can also be wrong. You know, the wrong model, the wrong equations. It can be wrong, so you need both systems. But the question is, you know, if there is this extreme fear -- And by the way, I think that we see that there's a similarity between the way the government is responding to terrorism, with all its analysis, and the way the public is responding. They're kind of in synch. That's why the public tolerates so far this massive expenditure to deal with what Professor Mueller says is a very small risk. It's because it's in synch with the way they're responding.

So how do you dampen what might be these strong fears? Again, I think the issue of control, you have to -- It's an emotional response, so I think there's two aspects. Give people a sense of, if this is not uncontrollable, that authorities know enough and are doing enough to control it "and there are things you can do as well." That can reduce the fears.

The other thing that can offset fear is benefits from certain activities. I'm not quite sure how that would play out here, but risk and benefit blend together, and the benefits can offset the risks.

One last comment on what we're talking about here is the issue of hindsight. One of the reasons I think the government is doing so much is that they know that if they aren't seen as doing everything possible, then if something does happen in the light of hindsight, which we know is a real powerful, biasing factor, they'll be crucified, and they don't want to run that cost, so we have to try to get the government not be so vulnerable in that sense.

PROFESSOR MUELLER: Usually the initials are CYA.

MR. ROSENZWEIG: You just described Washington.

John Sabo.

MR. SABO: I think it was Professor von Winterfeldt talking about vulnerabilities, consequence, and probabilities. And consequence is the easiest or, at least, most readily addressed. When you think in terms of privacy, privacy isn't a mathematical issue. I guess you could develop some models for determining consequence of impact. But if you look at things where you have very complex systems that are interacting and those

interactions create additional complexity -- for example, using data from different sources, combining it, making decisions -- do you have any recommendations about how one approaches doing a reasonable job risk assessment in this sort of softer space? It's not mathematical; you're not looking at trajectories or chemical composition; you're really looking at the personal information and the values that people have. Do you have any views about approaching risk management and privacy in the privacy arena?

PROFESSOR VON WINTERFELDT: Well, I haven't given much thought. I'm speaking a little bit off the top of my head here, but my inclination would be to focus on the pragmatic impacts to people, as opposed to the abstract protection of privacy. That's how I would approach it in the first sense.

So what does it mean to me if my privacy rights are violated? Is it just a violation of privacy? freedom? or is it something that has tangible consequences for me? And I would count the tangible consequences. I think that's at least one handle you can get on it. Of course you want to protect these principles as a matter of cause, but in terms of analysis data on privacy impact assessment, I would first look at how many people are affected, what is the effect that occurs, how serious is the effect, and, if it occurs -- for example, being arrested erroneously -- how can we make up for it in a speedy manner? So I guess I'm a bit of a pragmatist in this area.

MR. ROSENZWEIG: Joe, you're next.

MR. LEO: I trumped you, Joe. I'm interested in having this expert panel help me and help the Committee in lessons learned on risk assessment and our recent disaster Hurricane Katrina in New Orleans, which I am told -- Now, I haven't read the reports, but let's work on the hypothesis -- several years ago when all these great experts did risk assessment, risk analysis, risk everything, published big reports, said what would happen after a hurricane Category 3 or above, blah, blah, blah; here we go, boom; now we've got a $100 billion disaster.

So my one remark to Professor Mueller is that I'm not so sure I'm ready to embrace your paradigm that -- I mean, the risk is there or the risk isn't there, to some degree, and we're spending all this money because my affective -- my emotional side says, "Hey, man. Here's a whole bunch of people who are willing to give their lives, to strap their bodies with C4 explosives, to blow up people in the process." And then there's a new paradigm and it seems like -- I watch the television, and there's a lot of people who hate us.

So I really do feel potentially there's a risk there, and I'm trying to get a lesson learned from what we knew -- All the assessment that we knew about it and we did not take, apparently, the corrective action in the case of the hurricane and now we're spending billions of dollars on the terrorist threat. Is there some lesson learned from what we just

went through to what we might do better or different in this terrorism paradigm that we now are now confronted with.

PROFESSOR MUELLER: Let me make just a few points on that. As you're probably aware, there's been quite a bit of criticism on the Department of Homeland Security in the fact that it's spent huge amounts of money on trying to get first-responders and so forth to deal with things which haven't happened, which is biological, chemical, and nuclear attacks, and very little, by comparison, on natural disasters and so forth in case something does happen.

And I don't know the depth of whether that criticism is valid and so forth. But there were huge amounts of money being pumped into things which might well have been better spent on preparing for things which actually are going to happen.

In terms of dealing with the occasional terrorist act, I think it's hopeless. If anybody wants to blow up something, they can do it. You, basically, can try to prevent it, but you can't predict everything. You can't protect every barn, every McDonald's, every bridge, every railroad track, every road, every monument; and if you do, following up on what Professor Slovic said a little bit ago, there's the Washington monument, and they're now trying to protect that, so the terrorists will say, "Well, where else can we find something large and funky that we can blow up," and they might come to Seattle.

So it's just extremely hopeless. There's just no way you can protect against every possibility of that sort. And it seems to me that instead of spending money trying to prevent everything -- Every bus? You know, after London. Anybody with a backpack can blow up a bus, right? Do you want to protect every bus? every mile of highway? every inch of railroad track? It's basically hopeless.

So, consequently, instead of trying to do that, which strikes me as an exercise in spectacular futility, it might be better to just store away the money, and if things do happen -- and they don't seem to happen very often -- the track record is not extensive -- is to then use that money to fix it when it happens and then go after the perpetrators once they have done it.

I guess that's kind of a pessimistic way of looking at it, but it seems to be realistic, at least to me.

PROFESSOR SLOVIC: I think the comparison with the hurricane is instructive because one of the things that's been known about risk perception for a long time -- in fact, the earliest risk assessment studies were with natural hazards in areas of flooding and earthquake. And this was 60 years ago. A geographer pioneered this work.

And what he observed was that -- and has been repeatedly confirmed, is that we don't respect nature as something that can harm us. Nature has a very good public relations deal going. Nature is benign. The word "natural" is a very positive concept. We

don't fear nature. And the history of human response to natural hazards is always to kind of underestimate. When the hazard hits, you then respond to the crisis. You kind of shore things up based on what happened, expecting the next one, if it ever occurs, will be just like the last one.

You go back and repopulate the area. It's happened over and over again. We don't dread natural hazards. We dread -- Again, it shows the difference of this psychological dread aspect. We don't dread nature. We dread terrorism.

PROFESSOR VON WINTERFELDT: The experience with the risk assessment part and maybe to some extent the risk management part, the levees in New Orleans, I think, is very indicative of the failure to translate the findings and results into political action. I mean, if you look at the studies, they actually went all through the steps that I went through, all the way up to evaluating alternatives and concluding that something needed to be done, to the tune of, I think, several billion dollars, not a hundred billion. And it was done.

So my conclusion in those situations -- And I see this often -- I see this also in the earthquake field -- that good, sound proposals for pre-event mitigation are ignored because money cannot be set aside for these speculative purposes, if you will, and that you as a risk assessor have to actually become part of the action. And I've done that in a few cases where I was especially convinced that something ought to be done, and it's tough because you're sort of stepping out of the analytical world and you essentially are becoming an actor.

I never assume that whatever the assessment says is the right thing. I do believe that the perceptions and emotions on -- It's one thing to throw into the political debate, which is usually messy, but if you don't throw it in and you don't throw it in with some muscle, it's not going to be heard.

MS. LEMMEY: First off, I'll start off with a very quick story last week in San Francisco. The Chronicle ran an article -- I think it was a FEMA study.

There were three things that would hurt the economy -- a terrorist attack, breach in New Orleans of the levees, and then the "Big One" happening in San Francisco. And we all looked around the table, and the New Yorker was like, "You guys are next." And we were, like, "Bummer. We thought we were first. We were ready." I think there is a real attitude issue that's in places where people are more prepared for it psychologically, a very different state of mind.

I have two questions sort of on point to the privacy issues. The first one is, I have been doing a lot of work -- not on this commission -- outside this commission on information sharing in the government, and we have been looking at risk assessment on

the risk of not sharing what happens, because, as we learned from 9/11, it was the risk of not sharing information that prohibited activity.

Well, what we're finding is, because on a -- They did a model -- On a need-to-know model, there has been less and less sharing. Where this comes into the privacy problem is it still creates a lack of transparency of the information. It still moves people into a classification scheme or a fear of exposure that forces the privacy problem to behave differently, because we cannot get the kind of exposure oversight and transparency requirements that are there because they're overvaluing the risk of exposure of this information. So I'm wondering if any of you-guys have run into that along the way and how we might want to look at that.

And the second question I have is: Because we hear from you about this escalation -- this fear requirement -- What we've seen in public policy historically is, the second something happens, all the rules go out the window.

If we can anticipate this fear response from a privacy perspective and a civil liberties perspective, how do we think about proactively looking at policies that don't allow people's heightened sense of response -- just sort of throw everything out of the window the second we have any kind of a purgation in the system.

PROFESSOR MUELLER: People may react violently, but as I suggested earlier, it doesn't mean the government has to do so. If smoke and mirrors are certainly an indication that you're on the case and so forth, that may be enough. If the fear is really something that's being substantially exaggerated -- or the probability of the threat is being exaggerated, there's no way to stop people from being alarmed. I mean, it's going to happen, I suppose. It's very hard to predict, though, it seems to me.

But, you know, in the United States no one seems to be concerned about global warming, but in Europe, they are. In the United States, people are worried about nuclear power, but in France, less so. It's a very strange phenomenon.

In the United States, for a long time people weren't worried about nuclear power, and then something happened and they became worried. I find it very hard to -- Looking over these things, there's a lot of places where you think people should have been scared, and they weren't.

The big thing is asteroids. Why aren't people afraid of asteroids? There's a very good chance -- one chance in 50,000 that one's going to blow up the world in 50 years. And it's precisely calculated. There's been thousands of movies about that, going back to H.G. Wells and so forth. And it's got all the things that -- Paul Slovic talks about it. It's dramatic. It's uncontrollable. That kind of stuff. And you can't get people to move. Now, maybe there'll be a new mobility.

Chicken Little is coming out in a month or two, in which the sky really is falling. And maybe then people will start to get hysterical about asteroids, but I doubt it.

MR. ROSENZWEIG: I watched Armageddon, and if that wasn't enough to scare everybody, I don't know what is. Does anybody else have more questions?

PROFESSOR SLOVIC: I don't feel I have good answers, but with regard to -- I think about this discussion in reading the consequence, reading the Framework document, I'm just sort of wondering about these various aspects of privacy; that is, in terms of "What is at risk?" We hear terms like liberty, freedom, self-determination, control, and fairness. And I just think in terms of modeling the impacts. I mean, what are people's values here? I mean, we throw these terms around and we treat them with great respect, like freedom and liberty and so forth, but, I mean, what are people willing to trade off? What are our values with regard to, you know, these concepts versus certain benefits from security? How much are we willing to give up, one type of benefit to gain some security? And I don't know whether people can answer those questions or where they're at, but it seems to me that's kind of fundamental to policy-making here, especially if you're going to do it again. This risk framework, it's not just risk; it's also benefit. Well, what are these benefits? What am I being threatened by here? I think this is a question that needs investigation.

PROFESSOR MUELLER: Very briefly on that. After 9/11, there was obviously a willingness to give up privacy rights and so forth. The Patriot Act passed 99 to one, or something like that. But it might be a good time now to suggest, you know, what good did it do us? I mean, the whole point of things, we obviously want the police to be able to find the bad guys. Well, they have been looking for four years, and they haven't found any.

So maybe we can get those rights back because it didn't -- you know, we're not getting anything for that. If they found all kinds of terrorist cells all over the country, then maybe you could say, "Well, maybe it was worth a deal." If you pay something and get nothing for it, it suggests that maybe you should not have to make that payment further.

PROFESSOR VON WINTERFELDT: I would endorse what Paul said. And just maybe coming again from my rather pragmatic view of these things -- and I mean that in a philosophical sense, not just in a practical sense -- that we have to shake out what we're protecting, why we're protecting it. And I think the worry -- From my perspective as a citizen, the worry is not about privacy as an abstract concept. The worry is about misuse of the information in the wrong hands, in government or shared by others that I definitely don't want that information to be given to. If we could better understood what we're protecting in terms of the values people have regarding privacy, I think we could do more in terms of making these tradeoffs and addressing the more practical issues of what is being impacted if you violate all those privacy measures.

MS. McNABB: I wonder if you would be willing to give us some written comments on our Framework document. If that wouldn't be asking too much, we'd appreciate it.

PANEL MEMBERS: Sure.

MR. ROSENZWEIG: We'd appreciate any feedback you could give us that might improve what we're doing.

PROFESSOR SLOVIC: You might also contact or have testify some folks in high governmental positions who have a lot of experience with risk assessment. I'm thinking, for example, of John Graham. He used to run the Center For Risk Analysis at Harvard and is now the regulatory information czar or something like that. Another person is Dick Meserve, who was the former chairman of the Nuclear Regulatory Commission. Very, very, very familiar with risk assessment and uses and misuses of the government. There's probably somebody in the EPA. I know Dick Morgenstern was in the policy office. But somebody like that.

MR. ROSENZWEIG: That's a great suggestion.

Thank you. Joe. The other Joe.

MR. ALHADEFF: You had mentioned kind of it would be good to try to move the PIA earlier into the process when you actually had more rather than less options. In a pragmatic sense I would agree with you, except a PIA done right takes quite a lot of resources and quite a bit of time.

Are there some measures in the risk analysis and risk management world that may be kind of a more gross and less fine-tuned nature than a full PIA that could be used earlier on in the process? And that wouldn't negate the fact that it still is probably good to have a hygiene system of how you build privacy in at the get-go without having to worry about it but a way to test the options that are available early in the process but not with, perhaps, all the overhead of what a PIA may entail.

PROFESSOR VON WINTERFELDT: Well, I don't know how much time and effort and money you're talking about, but relative to the time and effort and money that DHS and other agencies typically spend on all these other aspects of shaking out the alternatives. Take MANPADS, for example. They're currently spending a hundred million dollars on evaluating MANPADS alternatives. That's a fairly clear -- I don't think that has a lot to do with privacy, so I don't think it's a good example for privacy. But it's a good example for spending a hell of a lot of money on assessment. So adding a million dollars for privacy doesn't seem to be outrageous to me.

Let's say a percentage of the funds that are being spent on regular assessment that should be spent on assessment of unintended, indirect, and some of the softer aspects of the impacts that the alternatives would have. Makes a lot of sense to me.

Now, the other question is, yeah, of course, sort of that if you can't do a full-fledged effort at the front end, I think anything else helps to do a qualitative assessment and -- You know, simply the sheer number of people that are being affected by this and how deeply they would be affected if things go wrong.

But at the tail end of all of this, you suddenly have this option on the table and all you can compare it to is nothing, and usually there is a large ground swale behind this option. There are advocates. There are champions. There are people who want this option. There are industries standing in line to implement it. So you can only fine tune it. You can tweak it. But you can't really look at others that have great benefits.

I have seen this in completely different context in siting energy facilities where the environmental part usually came at the very end. You shake it out after you decide which site you really want, as opposed to when you look at it in the front, you say, "Well, let's balance all of the aspects at the same time.".

MR. ROSENZWEIG: It's perhaps appropriate to mention because we focused on the Framework document, the Framework subcommittee didn't get to report to the Committee that one of the projects they're going to be looking at moving forward is ways to embed privacy earlier into assessment for the procurement process; you know, creating privacy -- entry points for privacy that are earlier than after at the end of the PIA, and they're going to do an analysis of the whole procurement, and actually after today, I'm thinking of the research chain as well and how to fit privacy into that better and make some recommendations. So if anybody's got any thoughts, we're interested.

PROFESSOR VON WINTERFELDT: This whole concept, the most recent National Academy of Science's study called Risk Characterization, I believe, promoted the concept of analytic deliberative processes where you interlink the analysis, risk assessment and risk management, with dialog of the stakeholders. This is another document you might want to take a look at.

PROFESSOR SLOVIC: It's called Understanding Risk: Decision-making in a Democratic Society. It's the International Academy, 1996.

MR. ROSENZWEIG: On the to-be-read list. Ramon.

MR. BARQUIN: Your comment of the probability neglect sort of had me thinking on the other extreme: Lottery, which is where nobody really cares what the probability is. However, going back to the dread, which is, of course, directly linked to fear, fear being that human reaction to a situation that we don't know how to react to. And what we do know is that if we are taught in some way how to react -- you know, like in the military, how do you react when you come under fire -- then we stop being as afraid. Not that we lose the fear, but we stop being as afraid.

The question here is, specifically on the privacy side, if there are some harmful consequences in some case, can we not, through education, sort of teach people how to react, when there is a false-positive and you are dealing with that at the airline station and this is what you have to do -- one, two, three -- and then you can react to some things like that on the privacy side. Anyway, that's a question for Dr. Slovic.

PROFESSOR SLOVIC: I certainly think that there are. Again, this is a point that Detlof was making about redress, that somehow there's fair treatment. Okay, if a mistake is made, then how can that be compensated or mitigated? You know, it's an aspect of remediation.

So, sure, I think that we need to consider what we can do through education and -- you know, but we have to start to do that. I don't know if much effort's been done to do that. I also agree with your point about the lottery. Lottery is a very excellent example of probability and neglect. When the jackpot gets up to about $300 million, people stand in line, even though the odds are maybe one in 80 million, because they get confused. The size of the jackpot confuses them about the odds.

MR. BARQUIN: There is one term that I have not heard from your side and I always thought was the key factor in mitigating risk, and that's insurance.

PROFESSOR VON WINTERFELDT: Well, the thing about insurance, my personal opinion is it's a vehicle to restrict risk, not to mitigate it.

PROFESSOR MUELLER: Terrorism is the outset of the lottery. What people say when they enter the lottery is, completely irrelevantly, "My chance is just as good as anybody else's." Now, I'm talking about the one in 80 million, and in the case of terrorism it seems to be the same thing: My chance of being killed is just the same as anybody else's even though the relevant thing is, "What is that chance?" Not "Is it the same as everybody else?" By the way, one possibility to deal with this, to bring up all the bad predictions that come out of this.

Do you remember last year, 2004, we were going to have terrorism at the Olympics. The only terrorist that showed up was the guy in a kilt who tried to stop the marathon. We were going to have terrorism at the Democratic convention, terrorism in the Republican convention, terrorism in the campaign, and terrorism at the election. When it didn't happen, people said that's because they weren't ready for the election, but the next six months are going to be really terrible. And what happens is, people don't remember those predictions.

In many respects the most important thing they try to develop is complacency. People are complacent when they get on airplanes; they go to restaurants; they don't give into terrorism. What terrorists most want is the overreaction and the fear. So one way to stop terrorism is to not be afraid. Lots of luck, however.

MR. HARPER: I thank you, panelists, for coming all this way and devoting all this time. I didn't have many doubts that we would get good information from you, and I have been more than validated in my suspicion in that we got a lot of good thinking and information from you.

Brief observation just for my Committee members, I recall when the London bombing occurred, Secretary Chertoff, being on one of the cable channels -- and my memory obviously just distilled to something that is maybe close to what he said -- but the essential message that he had is something along the lines of, "We will learn from this." And I thought that was a good example of leadership, a confidence-building message, but I feel even more so now given that I've thought about some the alternatives he could have said.

If he had said, "London should strike back," I think that would have caused people to exaggerate fears. If he'd said, "Let's start searching rucksacks," I think that would have caused people to exaggerate their fears. Likewise if he had said, "Avoid public transportation," or if he had said "Continue to use public transportation," that would have caused people to exaggerate risk. So now I'm absolutely delighted by what I heard from Secretary Chertoff.

MR. ROSENZWEIG: One of the other things he said was "We can't protect against all risks, so we can't spend billions of dollars to make the New York City subway safe," and the immediate reaction was from the Congressmen and Senators from New York who essentially said, "You must be crazy. You've got to make us safe." So he --.

MS. LEMMEY: -- said that they are searching rucksacks in New York.

PROFESSOR MUELLER: That is essentially an ineffective technique to try to suppress that -- But there's been no terrorism in New York since, so it must have worked, right?

MR. HARPER: My question is this, and it's one that I have seen bubbling up a few places in your writings. Let me pose a hypothetical to you.

I have a response to terrorism that is very expansive, that has substantial privacy consequences, that does not actually suppress a risk, but people think it does. Put it on any scale you like: good/bad, ethical/unethical, wise/unwise. Should we do things that make people feel good but are ineffectual?

PROFESSOR MUELLER: Yeah, if they're cheap.

That's a very difficult question, obviously, because of the first provisions of that. Looking for things that make people feel safe, if it's cheap, fine. You know, you have guys with Uzis walking around after 9/11, walking around in airports. If that really made people feel safer, well, I guess it's there.

We should probably be studying -- There should be two lines. One you have to take off your shoes, the other you don't have to take off your shoes, and see if the people who have to take off their shoes actually feel safer. If not, then you don't have to do that. Studies are being done. In Florida there was a case where there was a shark attack, and they promoted something forbidding the feeding of sharks. Now, if that actually reduced fears of sharks, then that was definitely cost-effective. But, yeah, I think cheap measures that reduce fear are fine for me because I think fear is the big problem.

MR. ROSENZWEIG: With that, let me thank the panel very much for -- When Jim and Joanne set this up, they said it would be educational, and I was put in mind that my father once told me if I learn one new thing a day, well, then I'm set, and you-guys have set me up for the rest of the week as well.

We now turn to our public speaker sessions. We have three people on the list, and our rule is three minutes per apportioned to the speakers. So I'll ask each of them to come up and take three minutes of their time to say whatever they wish. And the first, certainly no stranger to the members of the Committee because we saw him in Boston, Bill Scannell.

MR. SCANNELL: Mr. Chairman, thank you for allowing me to make a few minutes' worth of comments.

First I'd like to congratulate the organizedness of this meeting, for holding this rather expensive thing in a remote luxury resort, far from most international airports in this country. It's not only made sure that the attendance on the part of the interested parties and activists were next to minimal, but I believe there was only one journalist here, who was a stringer who just happened to be located in Bellingham. So for future quarterly meetings, might I suggest the island of Guam; Adak, Alaska in the Aleutian Islands; and Penobscot, Maine. I think -- I think all three of those locations would continue this policy.

Also, it might be possible to publicly release the actual cost of holding this meeting in such a remote, difficult-to-get-to, far away place.

My second point that I'd like to make has to do with my disappointment in the Committee for, once again, giving TSA in general and Justin Oberman in particular yet another free ride. In Boston, he lied to you. I mean, the fine Saxon word "to lie." He lied to you regarding the use of commercial data in Secure Flight, and this all came out not only through their own way-back machine new Privacy Act edition but was confirmed by the GAO.

It disappoints me when we have such an opaque program where those of us who are not privy to the information that you have, nor have the platform that you have, have

to continue to dig for information, and yet when you have it before you, you simply don't ask the hard questions.

TSA has a FEMA problem. I mean, from Justin Oberman right on down to -- there is no one in his department that has any security background whatsoever, and yet when he comes before you two and a half years after working on a program that has gone absolutely nowhere, we get the Committee version of "You're doing a heck of a job, Obermanny." And I find this very upsetting.

And thirdly, I'd like to address Nuala's leaving. Nuala O'Connor Kelly I have a great deal of personal respect for as a human being, but the fact is, she was stuck in the unenviable position of having to work internally to try and stop privacy invasive programs before they came out and to do fire-watching that way, while, at the same time, acting as a quasi advocate for members of the public, such as I and the rest of our citizenry, on issues of privacy relating to Homeland Security.

It's a very, very difficult circle to square, and unfortunately, in my perspective, she ended up doing nothing more than being flak-absorption material for very, very poor Homeland Security policies, those of TSA's in particular; and one can hope that you-all will help strengthen not only the role of her successor but the transparency of what's going on with these programs in particular, because the idea that 18 criminals who are foreigners can turn us all into suspected terrorists and having our names run just to simply be able to freely travel in our own country, I find it un-American. And I think as our colleague, the professor from Ohio, quite rightly pointed out, that when we find this acceptable, that the terrorists truly do win. And I thank the Committee for your time, for my time.

MR. ROSENZWEIG: Thank you very much.

Doug Klunder.

MR. KLUNDER: Thank you to the members of the Committee for allowing this comment. I am Doug Klunder, and I represent the American Civil Liberties Union. I would like to just make a couple of comments about Secure Flight, following our very public positions in the past, so nothing I say will come as a surprise to you.

We are very pleased that TSA has apparently backed away from the use of commercial data, but we are very concerned that it is -- the only thing TSA has said is that they will not use it initially but no guarantee that it will not be used in the future, and Mr. Oberman today seemed to indicate that it was merely a matter of priorities.

So we very much believe the use of commercial data should never be allowed. We're worried about TSA's history of misinformation on the use of data and fear that any future use could once again fall into that trap of not complying with Privacy Act and not informing the public as to how that data is being used.

That's of particular concern because of the broad scope of the Secure Flight program, while protecting against known and suspected terrorists pretty much is open-ended, and so that really is not any constraint on the use of commercial data.

I would urge this Committee take a stronger stand than you have already taken with the report you issued today talking about the dangers of commercial data by -- Rather than simply saying issues that should be kept in mind than procedures that should be followed, we would much rather see a flat prohibition on the use of commercial data. Not now. Not ever.

And then my second point I'd like to address, going beyond commercial data, Secure Flight overall is a serious problem, and it's not merely privacy advocates who are finding this. When every governmental organization that has taken a look at Secure Flight or its predecessor CAPPS II has come up with the same conclusion, that it's not working, the information isn't there, it's ineffective, and our unanswered privacy problems, seems to me that it's time to reevaluate whether Secure Flight should be proceeding at all. It's expensive. It's invasive. And it's ineffective. We reiterate our opposition to Secure Flight.

Thank you.

MR. ROSENZWEIG: Thank you very much, Mr. Klunder.

James Harrison.

MR. HARRISON: Thank you very much, Committee. My name is James Harrison. I'm a private attorney, and I represent, among others, John Gilmore, in Gilmore versus Ashcroft, Gilmore versus TSA and four Alaskans that made Privacy Act requests for commercial data back when TSA was saying they weren't collecting commercial data.

It's unfortunate that you-guys have the job to do privacy analysis and kind of at the same time be lied to by the TSA. Jim Harper's question to Mr. Oberman when Mr. Oberman was pressed to come clean about what commercial tests they had done, he said, "Well, it's over and we have only done 90 days of tests" and whatnot.

Jim asked for the contracts that TSA let on that project, and through my own investigation I've been able to find, using government databases, the initial contract was issued in February of this year, and there have been four amendments to that contract, the last amendment being in August, and the operation of that contract is to go on into October. So I'll provide that to Mr. Harper, and perhaps he can pass that on to the rest of the people.

MR. ROSENZWEIG: Actually, I'll ask you to send it directly to the Privacy Office so that it can be circulated to all of us and be put on the web, unless of course there's some reason you want to give it to Jim.

MR. HARRISON: No, that's fine. I, again, used a government database, just looking for the contract, and there it was.

So anyway, with regard to Privacy Act requests, it's very difficult to legally evaluate privacy, as you know, and on one hand, you have the imposition, and on the other hand, you have the effectiveness of balancing. And the effectiveness here is extremely difficult; I mean, we're not being told whether it works, how it works, what the metrics are for testing that it works.

To just be told that the testing has been very successful and we're very, very pleased doesn't really help us at all. And one of the things that I've tried to do is to make Privacy Act requests for data contained within the system of records used to test Secure Flight.

And you'd think that Secure Flight, being a system used to find data, would be able to -- they would be able to deliver on our requests for this data, but they have been both unwilling and unable to do this.

We've provided names, date of birth, place of birth, and place of residence, and they haven't been able to come up with data in their system of records. And then they come back and said, "Well, you need to tell us the airlines that you flew and when so we can find it." And they have not found anything. And particularly disturbing is that they haven't found anything in the commercial data, with a hundred million records of some unknown sort.

Not only that, but they have somewhat ignored our requests, and I have had to go to the courts to force them to respond to previous requests. I have a case pending presently up in Anchorage.

As a result of these requests, there have been hundreds -- these are requests of my clients -- there have been hundreds of requests now made with the aid of organizations such as -- (indiscernible). You can go to their website. They're trying to sort of reverse engineer this system of records to see if -- you know, what they're doing, is it effective. We're dealing in a darkroom here for effectiveness.

And TSA has come back now and again requested the airlines flown and the dates, but they also want to know the phone numbers that people have left for the airline to contact in case they need to -- you know, to be able to search this data. This data cannot be searched automatically. It must be searched manually. What's going on here? I mean, are they going anywhere with their tests? They have spent a hell of a lot of money on this, and if they can't just respond to a simple Privacy Act request, how are they going to do Secure Flight? They've also requested now that people prove their citizenship when making Privacy Act requests, and if they don't do it within ten days, they're going to round-file their request..

I saw also that you've put together a conceptual proposal for addressing Privacy Act requirements. I ask that you might consider, when considering your conceptual proposal, that, you know, put the fire to them a little bit on Privacy Act requests and make them comply with the law.

Thank you very much.

MR. ROSENZWEIG: For what it's worth, the man leading the charge on that is busy taking notes. So hopefully -- The conceptual proposal, John will be our liaison on that, and he's busy taking notes. So hopefully that will help.

We've reached the end. I suppose it is worth saying that we are here because the border is here and the Department is trialing a lot of very interesting and challenging new technologies, including radiation detectors and RFIDs, just a few miles from here, and part of the Committee's task is to understand those new proposals, not in theory but in practice.

It would have been our wish, Mr. Scannell, to have held this meeting in Vancouver, a much more readily accessible city. It turns out that's not permitted under Federal law, so the only other option would have been for the Committee to basically drive all night back to Seattle -- or up from Seattle and back, which would have measurably reduced the utility of the event for us.

It certainly is our intention to hold our meetings in a public forum available to everybody. The next one will be in Washington, which I'm quite sure we'll be able to get you to. And we'll move on from there.

Before we adjourn, I would like to thank the staff of the Privacy Office for putting together two days here, Maureen Cooney, Erica, Peter, Ken, Billy, Nathan, and especially Tamara Baker, who does all the travel arrangements for us, and our Designated Federal Officer, Rebecca Richards. Without their work, we could not have had the informative and instructive two days that we had here.

And I want to thank all the Committee members for their attention. I want to thank all of the witnesses and the members of the public for their attendance.

And did you wanted to thank somebody, Howard?

MR. BEALES: No. I just wanted to reiterate something that you seem to be leaving out.

MR. ROSENZWEIG: I hadn't finished yet.

MR. BEALES: And that is that, you know, as we move forward in looking at Secure Flight, in particular, and all of the things we're looking at, in general, that comments from people about exactly what we ought to be asking are relayed through our website are something that we would certainly be delighted to consider and look forward to

considering as issues that we ought to be looking at. And that opportunity is there, and I hope people will use it.

MR. ROSENZWEIG: That invitation applies not just to our inquiry about Secure Flight, but examination of the Privacy Act, examination of the Framework principles, the procurement process, and whatever else it is that we've mentioned that I've forgotten over the course of this day. With that, I will adjourn the meeting. We will reconvene on Tuesday, December 7th --.

MS. RICHARDS: December 6th.

MR. ROSENZWEIG: Tuesday, December 6th in Washington, D.C. at a place to be announced in the Federal Register. Thank you very much, all, for coming.

(Meeting concluded at 4:46 p.m.).