The Privacy Office
Department of Homeland Security
Privacy Office Workshop Series
Transparency and Accountability:
The Use of Personal Information Within the Government
April 5, 2006

OFFICIAL WORKSHOP TRANSCRIPT

Horizon Ballroom
Ronald Reagan Building and International Trade Center
1300 Pennsylvania Avenue
Washington, D.C. 20004

PANEL I
NOTICES - A TOOL FOR TRANSPARENCY

Moderator:

Toby Molgrom Levin

Panelists:

Eva Kleederman
Elizabeth Withnell
Amy Friend
Loretta Garrison
Martin E. Abrams
Paula Bruening
Alexander Dix

MS. LEVIN: Thank you, Maureen.

Good morning, my name is Toby Levin. I'm the Senior Advisor in the DHS Privacy Office, and I just want to echo Maureen's welcome. Workshops are always a wonderful opportunity to learn and share information, and I hope you will find this morning's panel a stimulating one.

I want to begin by expressing my own view that notice is absolutely the best way to start such a workshop. When we talk about transparency and accountability it does begin with notice. And a cliché, but a true one. I think that notice is fundamental. It's fundamental because of the Privacy Act of 1974, it's fundamental as a tool for government accountability, and it's fundamental for a way of informing individual members of the public about any rights they may have with regard to the use of their personal information.

So if we think of notice as an accountability tool then you can understand why it's important that it be effective notice, that it be meaningful notice. And what we're going to talk about today is how to make notices effective and meaningful.

I'd like to introduce you to our panel. We're going to -- we were going to begin this morning looking at government notices, but our kick-off panelist, Eva Kleederman, I think has been delayed. But I'll make the introductions and hopefully she'll be arriving shortly.

To give us an overview of notices in the federal state we've invited Eva Kleederman, who is Senior Policy Analyst with the Office of Management and Budget, Information Policy and Technology branch.

And Elizabeth Withnell who is Chief Counsel to DHS Privacy Office.

Then we'll hear from representatives of two federal agencies that have just announced the results of consumer research that they've done to improve financial notices, and those are the brochures and flyers that you've received from your financial institutions for a number of years now.

Amy Friend, who is Assistant Chief Counsel of the Office of the Comptroller, Department of Treasury, and Loretta Garrison, Senior Attorney, Division of Privacy and Identity Protection of the Federal Trade Commission. And their research is very exciting and has ramifications for notices in the private and public sector.

Then we'll hear from Marty Abrams who is Senior Policy Advisor and Executive Director of the Center for Information Policy Leadership at Hunton and Williams. Marty has been a leader in the private sector in developing better notices within the U.S. and internationally.

Following Marty we have the honor of hearing from Dr. Alexander Dix who is the Berlin Commissioner for Data Protection and Freedom of Information. He will report on

European and German developments regarding notices.

And completing our panel presentations will be Paula Bruening, who is Staff Counsel for the Center for Democracy and Technology. She's discussing the important of transparency through notices from the perspective of the individual members of the public and non-governmental organizations, and she may comment on how well we in government are doing with regard to providing notice.

After the presentations we'll have a discussion, and I hope a lively one with your assistance, on what we can learn from the research and experience of the private sector that maybe relevant to our work in the public sector.

I particularly want to welcome our international guests and my partners in other federal agencies who are working on notices and FOIA throughout the government. We will learn from you today I'm sure.

We will set aside questions at the end of each panel and to make sure that we can hear from you as well.

So I'd like to begin today, since Eva has not arrived I think we'll go ahead and begin with the presentation on the private sector. Let's see what we've learned in that state.

And, Pete, do you have the remote? No, private sector, we'll start with the government first, so we'll give it to Lori.

MS. GARRISON: While we're getting that loaded, I'm Loretta Garrison and with my colleague Amy Friend we represent two of the six agencies that have just completed the first phase of extensive in-depth consumer research. It was just released last Friday and we're very pleased to talk to you about it today.

We decided to co-present so that we can have an opportunity to describe our research a little bit more fully to you.

Two announcements; first, I need to give the requisite disclaimer, whatever I say today represents my own views not those of the Commission or of any individual Commissioner.

Second, I noticed when we were doing the hand outs for you that the website for the information on the interagency research notice research project does not appear very

clearly on your printout, but you'll notice it at the bottom of the screen here, and if you go to that website you'll be able to find all relevant documents on this, including the report that was just released Friday.

Amy?

MS. FRIEND: Thanks, Lori. This project that Lori has begun discussing has been a long time in the making, and just to tee it up I want you to know that Lori is from the Federal Trade Commission, I'm from the Office of the Comptroller of the Currency. And we worked so many hours together over the last few years that Lori even knew that I had broken window sashes on my windows at home, and in the spirit of interagency comedy came over and fixed them. So she's multi-talented.

I'm happy to talk today about this project that we put together on Exploring Alternative Privacy Notices that are easier for consumers to read and understand. And hopefully -- there we go -- what the objective was, was to try to come up with notices other than those that you may know today which sort of look like this, these multi-fold brochures that many of you may have seen and may have tossed in the garbage. And we know from survey data that people think privacy is important but they've had a hard time reading through these notices because they think they're too complicated, and too dense. And so it's not worth their while and they usually end up in the trash. And we were quite dismayed with that.

So we set about coming up with notices that consumers could more easily read, understand and use. Use to compare privacy practices across institutions, and use to limit their information sharing if relevant.

The genesis of this was that in 1999 Congress passed a law called The Gramm-Leach-Bliley Act, and the main objective of that law was to break down the barriers between associations with banking companies, insurance companies, and securities companies. But part of that was a whole title on privacy, and what that did was require financial institutions to notify their customers about their privacy practices and give them an opportunity to opt out of some of those sharing practices.

When the notices first came out, which was 2001, they were required to come out in 2001, there was widespread criticism about them. This is what I showed you, these brochures. A lot of people, including members of Congress, thought certainly the media, individual consumers were complaining that these things were just too complicated. I think part of the problem was when all these different agencies, we had eight agencies working on privacy regulations, the banking agencies, the Federal Trade Commission, the

Securities and Exchange Commission, we sat down, we put these regulations together and really it was almost an after thought we put in sample clauses, and we did it largely to show the industry that the notices didn't have to be too long.

But we didn't give a whole lot of thought to it. So we came up with clauses like this, we do not disclose any non-public personal information about our customers or former customers to anyone except as permitted by law.

Or, we may also disclose non-public personal information about you to non-affiliated third parties as permitted by law.

And we thought terms like non-public personal information and non-affiliated third parties were household terms. They were in my household but they weren't in most households, and so this ended up leading to sort of widespread discontentment.

So what we did was we talked amongst ourselves and said we've got to do something about it because this was a whole new sort of privacy regime, there had never been anything like this for financial institutions at the federal level and we were very disappointed about the results, and we realized that we were at least partially to blame.

These eight agencies that all had rule-making responsibilities for privacy rules under the Gramm-Leach-Bliley Act got together and hosted a workshop in December of 2001 to explore how to make the notices more effective.

We talked a lot about white space sort of design elements, punching up some of the paragraphs, bullet points, steering away from legalese. We didn't really get into the content of the notices. A lot of the industry talked about how the regulations were so complex, the statute was so complex, where relevant there were nine different items that need to be disclosed, and they said hey, you know, we've done the best that we could.

We also talked about the idea of a layered notice, that was the first time that I remember publicly discussing it where you might have a short sort of highlights notice that might draw consumers attention to important things in plain language, and then you would have a compliant notice that would accompany that that would meet all the legal requirements.

We heard from Dr. Alan Levy, who is the Senior Scientist at the Food and Drug Administration, who talked about the development of nutrition labels. And Dr. Levy explained how consumer testing was so important to try to find notices that actually worked and not just notices that people said they preferred, and what the FDA found was

that some of the notices that consumers said they liked better didn't perform as well.

I think this laid the seeds for what was to follow soon thereafter. I guess soon in terms of interagency speak because it was almost two years later. But what we did was -- let's see -- these eight agencies decided to issue an advance notice of proposed rule making to get some public comment about what should we do, that the state of the status quo was not acceptable and so how should we advance the use of, or the development of, simplified notices.

We asked for comment on standardization, on format, on language. We asked whether any consumer testing had been done, we asked for the results of that testing. And what the agency said was that before they would go forward and amend the privacy regulations that they would go ahead and conduct consumer testing.

So that is exactly what they did. Six agencies, this is the Federal Reserve Board, the Federal Trade Commission, Federal Deposit Insurance Corporation, National Credit Union Administration, the Office of the Comptroller of the Currency, and the Securities and Exchange Commission, funded a research project that has two phases. The first phase is complete and that's what Lori and I will be talking about today, which was really a qualitative study. It involved the development of form, of privacy notices, and then tested it on individual consumers to see whether they could actually use these notices.

The second phase that we'll talk about in a little more depth would be a quantitative phase with sort of a survey project where we take the results of what we got from this first phase and we evaluate it with a larger population of consumers to see whether it works for them as well as it works for the limited number of consumers that we tested.

And I'm going to turn this over to Lori to give you more information about the project.

MS. GARRISON: Thank you, Amy.

The project began in September of 2003 when after we put out a RFP we selected a local company called Kleimann Communication Group which has expertise in form development work and diagnostic usability testing which is a type of qualitative research. And in September of 2003 they came on board to work with us.

Qualitative research has many different components or methodologies associated with it, some of it includes focus groups. And focus groups can be very valuable in

learning, in getting impressions, in getting some preferences from consumers. They don't answer questions about content or usability.

For that we needed -- we conducted what's called diagnostic usability testing which consisted of very intensive one-on-one interviews that were 90 minutes long with individual consumers. We went to several -- about six different sites around the country and interviewed about six to eight consumers in each site. We were very skeptical at first when Susan Kleimann told us that after three or four you're going to know exactly what is working and what is not working with the notices, but in fact that held true at every single site.

Consumers are really very, very smart, and we put our heads together and came up with the best possible notices that we thought we could, and the first time we went out with a focus group they all bombed. We had to go back and start all over again.

So we went through some preference testing where we developed components for notices and tried to figure out for example what vocabulary they preferred, what they preferred in a title. We had different opt out forms, different disclosure forms, and we were trying to get a sense about some of them just looking at different pieces what worked. And after that we put a notice together and tried again.

We went through a pre-test and that bombed. So we went back and started again. And the first full round of diagnostic usability testing in San Francisco we found that we were onto something.

The testing was conducted as I said around the country. We went to San Francisco, Austin, Texas, we were in Virginia, in Baltimore, Maryland, Washington, D.C., Boston, Massachusetts and St. Louis, Missouri.

We selected people based on a number of demographics, we wanted even division on education, gender, race or ethnicity and income, as well as age. We were trying to get a cross section of people because these notices go to just about everybody in the United States, we're not talking about just one small sector.

So what were we looking for? We wanted to test first of all for comprehension. Does the consumer understand the basic concept of what this notice is and what they're supposed to do with it? Comparison, we wanted consumers to be able to understand how this particular company shared or used its information and how that compared to other companies uses of their information or their sharing.

The third thing we looked at was compliance. Gramm, Leach, Bliley is a very complicated statute, it's got a lot of complex information that needs to be delivered in a notice. On top of that it incorporates elements from the Fair Credit Reporting Act, and we also tested a newly enacted law, the Fact Act, which has a provision relating to affiliates. So we wanted to make sure that whatever notice we came up with met all of these legal requirements.

In addition to that we worked very hard to try and make the notice neutral and objective. The point here was not to drive consumer behavior, the point was to inform consumers, give them just the facts, ma'am, so that they could understand the information in front of them and decide for themselves what they wanted to do with it.

And we found that consumers really had used that range across the spectrum. Some don't mind the sharing, they love to get the marketing, others are more concerned and they want it restricted. Some prefer to get materials from affiliated companies as well as their own company, but they're not so interested in having their information shared with non-affiliates. So again the purpose of the notice was simply to present the factual information and allow their preferences to drive their own behavior, not to have the notice direct the behavior.

The note, we decided that it was important that the notices be paper based, they were not in fancy brochures, they were just simply on an eight-and-a-half by eleven piece of paper in black and white. They were in readable large print. The whole point here was that we wanted them to be able to see it, to read it, and test to see whether they understood it and can use it.

We also explored, as Amy said, a full range of options, everything and anything was on the table. Obviously with several false starts where things bombed we were looking for anything that we thought could work.

I'm going to step down here because I'm going to show you the notice and I'm going to leave it up on the screen even though you've got some other materials in front of you. I want to talk about them with the notice up.

The first thing is that in terms of major findings context was key to comprehension. We really needed to be -- we discovered that it you just gave consumers information about the disclosure, which in this case is the information -- okay, my little gadget is not working -- the information at the bottom half of the screen that if you just gave them that information they had no clue what it was or what to do with it. Consumers really do not understand about information sharing. So we needed -- the notice needed to also educate

them and give them a little bit of background so that they could get into the notice and understand what the notice was and how to use it.

The design elements then came after we worked on content to help aid comprehension, to present the information more clearly in a more easily readable and accessible manner.

The third thing we found is that when we worked with this design this notice allowed consumers to be able to compare across the banks.

Now the first think I want you to look at is the title. For those of you who can see it, it says Facts, What Neptune Bank Does With Your Personal Information.

Now missing from this title is the term "privacy policy," or "privacy notice." We learned very early on that those terms really don't work for consumers, not in the way that we wanted them. It put them off from reading the notice.

The terms meant to consumers that all of these documents said exactly the same thing, so what was the point in reading them.

On top of that they also thought that privacy policy meant that this is our policy, it's like a terms and conditions, take it or leave it, they couldn't do anything about it so they'd say well, yeah, thanks very much, that's your policy, right, now what?

So we had to get -- if we wanted consumers to read the notice we had to get away from that term, and it took a number of tries before we came up with this. Now what this does is it says "this is the facts, we want to engage you to read this notice, it's about your personal information."

The second part of this notice that's key is the upper half of the screen. This is called the key context information, or key frame. And this is the information that is very important to help consumers get into the notice.

You know, if you pick up a document somewhere or you pick up a book you might just kind of skim it very quickly and decide right away whether you think it's interesting or not interesting, worth your time to look at it or not. Well the same thing holds true in a notice. We needed to find words and sentences and thoughts that would bring the consumer right into the notice right away and make them realize that this might be something useful and important for them to read, and it meant that they could do something through this notice.

So it set up the framework for the disclosure table below. One of the first things that we see in this is the words "federal law." Federal law requires that the banks give you this notice.

That was very important to consumers, they felt comforted by the fact that the federal law in fact was regulating this area, that it mandated that the banks give the notices to the consumers so they could understand what was going on.

The second thing is that we described the personal information that was being collected. People didn't understand that it might be more than just their name, or maybe more than just their name and address. So we gave some examples of the type of information that in fact could be -- that was collected and could be shared with various parties. This could include your account information, your asset information, your investment portfolio, your account number, your social security number, all kinds of information. That was important for consumers to understand so that they could then make an informed decision about how they wanted that information to be used.

Then we come down to the disclosure box, which is really the key to the whole notice. We set this up in three columns, as you see. On the far left are seven reasons that a bank can share information. Now these reasons really break down into three categories.

The first grouping is what is this company, your company, what can they do, or what can it do? Well obviously it can share, and it does often, for what we finally came up with was everyday business purposes. They may have a mail house that sends out their mailings, they will have to report to the credit bureaus. They may have to file reporting -- or fulfill reporting requirements with state or federal agencies.

So all of these various activities where information may be disclosed are part of what the company has to do every day, and when people saw that and understood it then it made sense to them, they were fine with that. And every company will have to share that way.

Secondly, a company will share for its own marketing purposes. It may hire, again, a mailing house to develop and send out its own marketing materials. So that is the second one.

Third, under Gramm, Leach, Bliley the banks are permitted to enter into what are called joint marketing arrangements with other financial companies and they can jointly market. Again this is the company's decision to join with other types of financial

institutions to market products that they think their customers would like to have.

The second category has to with affiliates. If a company has affiliates it may share with those affiliates. And in our world of the FCRA and Fact Act it gets a little more complicated because it isn't just you can use this information, but it's in certain cases you can share transaction and experience information, but federal law doesn't permit an opt out there. A company could voluntarily do that, but they're not required to.

Then there's other information that is other credit worthiness information, that they may also share about you and in that case you do have a right under federal law to opt out.

The third element is the new Fact Act requirement which is being used for marketing. There a company may -- or an affiliate may already have your information because it could have received it, but this is a limitation on their ability to use it to market to you.

So these are peculiarities of the U.S. laws that we had to incorporate in this notice, but generally what you're talking about is sharing and use by affiliates.

The third category is non-affiliated companies. And in that case we simply set it up as their using your information for marketing because that generally covered the use in this particular situation. Here federal law does require in that situation that a consumer gets an opt out notice.

Now the second page of the notice is supplemental information that was useful to consumers but that they didn't really need in order to be able to work with the first page. We found that they could understand the first page by itself. The second page gives supplementary information but it also completes fulfillment of all the requirements that the law requires.

Here we set information up in frequently asked questions at the top of the page, and at the bottom we put in definitions for terms such as "affiliates" and "non-affiliates," "joint marketing partners." And in that case the company could also personalize under that, so if, in this case Neptune Bank which was one of the planet banks we were using, Neptune Bank shared fully, it had a lot of affiliates so it described the type of affiliates it has under that definition.

In another notice that we created called "Mars Bank," Mars had no affiliates, so it simply said we don't have affiliates, and on the first page in the disclosures they said we

don't share this way.

The third page is the opt out page. Now you get this page with a notice only if the bank shares in such a way that they have to provide an opt out. So as part of the development of the notice we came up with a form that included all ways in which an opt out could be provided, either by phone, by email, or by clipping off this form and sending it back.

And on the first page I forgot to mention that contact information was there at the bottom, that was absolutely key, consumers really needed to have that, they wanted to be able to know if they had a question who they could call.

I'm going to go ahead to page 19, and Amy will pick it up.

MS. FRIEND: Thanks, Lori.

I think in your packet of materials you all should have our slides and you might want to turn back to the privacy notice itself while I'm continuing to talk since we've taken it off the screen.

But as you saw in the first page it's this frame of the why, what, et cetera, why, what, how, followed by the table. And what we found was that consumers overwhelmingly preferred seeing this type of information about sharing and uses in a table format than they did in getting the same information in prose. We provided the same information but we took the table away, and what we found was that consumers no matter how smart or educated they were, and we worked with consumers, you know, sort of all over the lot, that they genuinely struggled when the information was just strictly in prose form to try to really delve into detail, and to compare it with other institution's sharing practices.

So what this table signaled to them was this is important information and they were able to read it. But one interesting thing we found was it's not just any table that works, this table worked well with the people we tested.

When we first started out with a tabular format there were some consumers that thought that they could change the yeses and nos in the column. So an institution might say yes we share, and a consumer thought that meant well we don't like that so you can cross out the yes, put in a no, and send it back to the institution so that they won't share.

Well in fact that's not what we were saying, what we are saying is yes, they share,

there's nothing you can do about it. But you might also have an opportunity to limit that sharing through the opt out, and if you look in your slides of our power point presentation you can see the different columns.

So one column is does this bank share, and the other column is can you limit the sharing.

So we had to work. I mean it was a lot of refinement. So again the table really seemed to reinforce consumer's ability to understand and to use this.

Let's see -- consumers preferred a larger and legible font size. We heard a lot from them that the notices that they're receiving in the mail the font is just too small.

As Lori said, we did it eight-and-a-half by eleven inch paper, nothing fancy, black and white and gray, no logos, but we wanted people to have no impediments really to being able to look at this and to read it.

As Lori said that page one was key information, it told them what types of information was collected, what types of information was shared, how they could opt out of that sharing. And people worked pretty well with that, but when we showed them page two which gave additional facts, it gave definitions, it gave some more context, it told them what types of affiliates they might be sharing with, what a joint marketing partner was, people said oh, we like that, okay, now we understand. It also told them about how their information was protected.

So people could work with page one, but said that they preferred page two and that it gave them a little more context.

Really what we found was that these simplified notices led to a much greater understanding, trust that the institution was being straight with them. One thing that we learned from Alan Levy, again the Senior Scientist for the Food and Drug Administration who also is working with this interagency group on this project, is that if consumers see a notice that's objective, like a nutrition label, they believe that it's factual, that it's not marketing, they trust what's in that nutrition label, they know it's mandated by the government and that what's in there is sound. And I think this table seemed to function the same way.

This is something that we learned about from the contractor, Bloom's Taxonomy. And it's different levels by which a person can sort of understand and synthesize the information in front of them. And what we found is that we as we went along in these

different sites that peoples' understanding increased and the way they performed in this sort of Bloom's Taxonomy scale increased over time as a result of making these refinements.

So when we started out in Maryland you can see that they were down around sort of the knowledge. What we found was that people were very good at navigating, they could find exactly where the information was in the notice that we asked, but when the put the notice away they couldn't talk about it at all, they were unable to really process it. So all they could do was say oh, yes, information sharing, it's over here in this notice. But they really exhibited very little understanding.

What happened was at the end of each round of testing the contractors came back and worked with the interagency group to make refinements to address what we saw as the obstacles to consumer understanding. And what you can see is by the time we got to St. Louis that they really rose through these ranks of this Bloom's Taxonomy and they could evaluate the information that was in front of them. So that was pretty exciting.

I am going to turn this back over to Lori who's going to talk about our key findings.

MS. GARRISON: Thank you, Amy.

Well I just want to quickly highlight what are the key research findings from this first phase of research that we have just completed.

First of all a contextual frame is absolutely vital to comprehension. Consumers when they get a notice need to understand what is this about, what am I supposed to do with it. So it needs to perform an educational function as well as a mechanism for drawing the reader into the notice to make them want to read it, so it's absolutely vital that this contextual information be up front.

Consumers want -- they'll tell you want a lot of information, but they want it in very few words. So the trick here is to find out what's absolutely essential and to make sure that that is only what appears in the key information.

Second, if you look at the disclosure table you present the whole in that disclosure table so that the reader can understand the parts. A consumer can look at the disclosure table and see at a glance how much or how little that particular company is sharing its information. So it allows for comprehension and comparability.

The visual presentation we found is far superior in organizing and presenting very

complex information so the consumers can understand it right away.

As Amy said, we tried our best to make a prose version, and it simply didn't work. We had some very, very smart consumers who read it, who worked with it, who could get the answers, but it really was a struggle. As the contractor said it was painful to watch them do it.

So the key here is not to make it hard, but to make it easy.

Standardization is also effective. Once a consumer has read that first page and understood it then they don't need to re-read it a second time, they know what that table is, they recognize it, know exactly how to use it and can handle it very quickly and easily.

Third, consumers need education about information sharing practices and the use of their personal information. They really did not understand this, and again this is why the key information is so important to helping give them that information to act on.

Trust. As Amy said we heard spontaneously from a number of consumers all across the country that they really didn't believe that their financial institution would in fact implement their opt out, they didn't trust them in the way they handled their information. A lot of them talked about the fact that they're just off selling it. So trust is a very important issue and transparency helps that.

Interestingly we heard that protection, particularly early on. When people saw the statement "we protect your information by employing procedural, physical and electronic safeguard measures that comply with federal law," another of our wonderful sample clauses, they didn't understand the second part of it. But when they saw "we protect your information," and then they saw how much of the sharing that was done they said how can you protect it when you're sharing. So it was a struggle for us again in this interest of objectivity and neutrality to come up with a statement about protection that talked about how the safeguards that are in place such as securing the building to make sure that the information is not -- there's no unauthorized access to it.

And finally, and I know, Toby, we've gone a little beyond our allotted time here.

We're into -- going to move into a phase two, we anticipate that it should take about a year. We hope less, we always hope less.

This quantitative research is going to evaluate and validate the findings in this first phase. We're going to be testing the notice that we developed in this first phase across a

much larger number of consumers, perhaps up to 2000, we're still working on the design. We'll also be looking and testing other current notices so that we can evaluate the performance of this notice. And we hope to have more information for you when we're done with that.

Thank you very much.

MS. LEVIN: We thank Amy and Lori.

I agree, much applause.

(Applause)

MS. LEVIN: This is absolutely astounding research, not only because it's being done by the government, which is -- when the government does research it's always a great thing, great steps in the right direction, but because this is ground breaking on how we communicate with the public. And so every time that Lori and Amy referred to companies I want you to go back when you look over those slides and think about the government because the government has the same audience. It's the individual members of the public, and it's also the broader civil society and all the NGOs and everyone who wants to know about what the government is doing.

So this research, my own personal view, is extremely important for us to look at and see how it applies, and we'll talk about that shortly.

But now we'll hear from Marty about the work that he's done in the private sector as well.

MR. ABRAMS: Thank you very much.

And first of all I want to congratulate Lori and Amy on the work they've done, the research they've done. As Amy would tell you if I weren't here I was one of those individuals who said your research is taking too long, you're not being transparent about what you're doing in your research.

I now understand why the research did take so long. I congratulate you for completing it, I would have enjoyed participating, so that the transparency issue isn't completely resolved. But truly this is the most important research that we've seen on how people learn from notices since the research that was done on food labels.

So I congratulate you on doing that work.

Toby is going to change my slides because I'm not competent enough to think about what I'm going to say and point at a screen at the same time, so Toby is actually going to do that for me.

And when I was listening to folks before we put together this -- when we were putting together the panel I thought it was important to take folks back to why it is important in a government setting for notices to be done well. And it really simply goes back to what we learned from Alan Westin back in the 1960s. And for those who have not read Privacy and Freedom in a while I would recommend you to go back to the first 40 or so pages of that book to understand sort of the context that which we need to think about privacy.

But in the simplest terms we are all in this continuing battle between society's need to observe us to create order and our own individual desire to have space where we can be who we are, where we can define ourselves, where we can reveal ourselves at the rate that we want to reveal ourselves.

And the government is really in the business of collecting information to make sure that things work, that they're collecting information for this whole concept of public observation. And this balancing act is critical and it's important, and transparency is the window to the public to understand if we truly are in balance.

And the first element of getting to that transparency is the notices provided by the government when it's collecting information or using information that it's collected by others. So notices are incredibly important in the government sector, in many ways more important than they are in the private sector.

I'm really going to go quickly over sort of the Center's notice project. I run the Center for Information Policy Leadership in 2001, the same year that really Lori and Amy began working on this project. We began to work on the project, and it wasn't just because of financial notices, it was because of HIPAA notices, it was because of the fact that notices on the web were going from one page to 12 or 13 pages, it was a general dissatisfaction with the ability of consumers to learn from notices.

So we formed a project, we decided it should be across industry, and eventually we decided it should be across borders and began working with international folks and international experts and privacy and education to make sure that what we learned here could help inform notices globally because increasingly commerce is global, and in some

ways even government processes are global. Just look at the issues related to passenger data coming into the United States to understand the globalization of these processes. So this truly is a global process.

And when we think about notices they really always have two purposes. The first purpose is as an accountability document, so the public can judge us to see that we are doing what we say we're going to do, that what we're doing is within bounds. So that requires a notice that is complete, the type of notice that Amy and Lori enjoyed reading back in 2001. The one with the model clauses. It helps the experts understand if an organization is in balance so that the experts can push back on the organization for its use of information.

But the second purpose is really for data subjects, citizens, consumers, people like you and I. It's so that we at a glance can understand how organizations are using information so that our behavior, the choices we make, can really begin to set the market straight in terms of what is the appropriate balance for using information to create value and to create protection.

So really it's important for consumers to be able to learn from notices, but the notice that works so well for the experts is not so that they can do accountability is not the notice that works well for consumers who are going to have to drive the behavior in the marketplace.

So we began to believe that the solution was layering, and we didn't pre-judge how many layers that might be. And I really think we've learned some about what layering means in the financial notice from the research that's been done here.

So we understand that notices have to be complete, but easy to understand, the complexity makes them hard to understand. Brief notices might be easy to understand, we collect your data, but they don't tell us very much, don't create the context for decisions, so that we really need to find a way to have a complete notice or to have notices presented in varying layers so the consumer can grasp what they want to grasp at any particular point in time. And I still believe that long notices have a value for the accountability process within organizations as well.

So there is a role for that long, complete notice.

Multi-layered notices offer a way for presenting information in layers so that all of the processes that are required by the notice can be completed.

The objectives of multi-layered notices would assure privacy notices are easy to understand, easy to compare and complete, very similar to what the U.S. government financial regulators were doing. That's achieved by communicating a privacy notice in layers. In some cases, for example on my PDA, if someone is collecting information maybe it's a three-line notice, and that's very important in the European setting. The standard is what in Europe is called the condensed notice, which is a template based notice with six boxes that convey much of the information that we were talking about before. And then there's a complete notice that is on request that has all the national requirements that might exist in the European setting, or all the requirements that might exist within HIPAA. For example in HIPAA there are over 30 required elements that need to be part of a notice.

So the concept is that you have layers, and that the layers serve a purpose. In the first case on my PDA it is alerting me to the fact that data is being collected by who, and what the general purpose is. The condensed notice gives you a snapshot of how information is being used, and the full notice has all the detail so folks like me can read them and say, that's too much, or hmm, that's just right, or they're not doing it -- they're not using the data consistent with the way they say.

If we go to the next slide I think this has really been confirmed by the research that was done by the financial services regulators, and it was really research that was done prior to the food label research, and it essentially said that there are three things you need to think about when you do a notice for consumers.

The first is that they need to be relatively short. The research back in the 1980s said no more than seven elements, that's what consumers can grasp at any one sitting, but you really need to be really short and pick the key elements that you're going to talk about. They must be in plain language, and by plain language I mean the language that I use across the fence with my neighbors. And if I use non-affiliated third party with my neighbors that's a cool word to use. But most of my neighbors don't use that word, so it's really got to be in any particular language that you're working the language that is used across the fence.

And it must be in a common format, and I think that's one of the things that the financial services regulators learned, that we need consumers to begin to say that is what a privacy notice looks like, I understand it's a privacy notice, I can go to the parts in the notice that I'm interested in, I can compare box to box. So we really need to have a common format for notices to work.

In terms of the condensed notice, and I'm going to ask you to flip to the next slide.

This is Proctor and Gamble's privacy notice. Next I'm going to show it to you in Korean. Most of the audience reads English better than they read Korean, so we're going to go in English.

You'll notice that the first it says who is giving the notice, what is the organization that is letting you know their privacy practices. In this case it's Proctor and Gamble, and then covers all of Proctor and Gamble's various brands.

The second is the personal information that I collect from you and from others about you, and again it's in bullet form, it's in short phrases, it helps the individual understand the types of information that are collected.

The third box is uses and it could be called uses and sharings. And it's the general, normal uses or uses that the consumer want to anticipate of that information, so you cover both.

As Richard Thomas, who's the Data Protection Commissioner for the United Kingdom would say, anything that's unexpected should be covered in this template form notice.

The next box is your rights and choices. In some it's just called choices, and this tells you in a national setting what your rights are. In many cases in the United States consumers don't have rights related to the collection of information, so it tells you your choices, things like your ability to limit sharing, your ability to gain access if the organization provides access.

Also very important to the right is how to contact us. We found that consumers typically liked more than one way of contacting the organization. And last is a box that's called other important information. Remember we're dealing with a very complex marketplace where there are differences from organization to organization to organization, and that box allows the organization to say what is different about the management of information at that particular institution.

Go to the next one.

This is the same notice in Korean. The fact is that you can get a Proctor and Gamble notice in over 40 languages. The fact is that if I had an MSN notice up it would look very similar to similar to this, the same boxes, but would talk about MSN sharing, and again that's in over 40 languages.

If you could go to LoNovo, that's in about -- it's at least in 20 languages. You could go to a number of organizations and you'd be able to see the same format but used from organization to organization, from language to language, the same format globally.

Please go to the next one.

Layered notices work for the public sector as well, and a number of the folks I worked with as we developed this international norm are data protection commissioners, are officials in governments, and a number of them have begun to adopt this concept of a multi-layered notice.

Please change.

This is the notice for the Australian government. This is the site -- when you go to the Australian government site this is the first privacy notice you'll find. Again it looks very similar to Proctor and Gamble's notice.

Change please.

This is the U.S. Postal Service. There's already a government agency in the United States that has gone to this norm of using this structure, and this was actually based on their testing because they really liked their long notice, but they found on the trust category this particular notice built trust.

Next please.

This is the New Zealand Privacy Commissioner's notice. Again, if you've seen the Australian notice, if you've seen the Proctor and Gamble notice, you know how to read this notice.

Change please.

This is the British Columbia Data Protection Commissioner's notice, again in the same format, the say way of laying out the information.

Please change.

I know a lot of you think that the compliance issues related to the Privacy Act are very complex, and I know a lot of you think that that privacy aspects of doing a privacy impact statement is very difficult as well. I would suggest that there are no more difficult

than the compliance issues related to GLB, GLBA, HIPAA or many other privacy laws. So that you can figure out a way to use this concept of a short notice or a condensed notice to help educate people about your organization's use of information in any particular setting.

Please change.

Along with international experts, and literally international experts, I received comments from New Zealand, from the United Kingdom, from Europe, from Canada, we developed something called ten steps to develop a multi-layered privacy notice. It is available on our website, and for those of you who don't want to go to our website I have 30 copies that I would be more than delighted to give away because I really don't particularly want to take them home.

And what this does is help you work through the process of developing a notice from scratch and then turning that notice into a multi-layered notice.

One final word. We all have to learn from the research, this is an evolutionary process. Part of the challenge that the folks that I work with and I have is to go back, take the research that we have seen on financial services notices where we really have seven defined sharings that we can all rally around and begin to figure out what that means for the notices that we've developed as we migrate them to the next stage.

And there are a couple of things that I have learned. One is that we truly need to tell folks why they're getting the notice. I think that that's an incredibly important change that we have to adopt.

The second is in the whole area of how we use information. I think that we need to find ways to make it clear. I'm not sure how we get to the tabular format that we saw for the seven sharings, but we need to figure out how to make the uses section present the key section much clearer.

Thank you very much.

MS. LEVIN: Thank you, Marty.

(Applause)

MS. LEVIN: And now Dr. Dix for an international perspective.

DR. DIX: Thank you very much, I'm delighted to be on this panel and let me start by saying that when I was first asked to cooperate with my colleagues abroad, and in particular Marty Abrams and then Malcolm Crumpton, the former Australian Privacy Commissioner asked me if I was interested to get involved in this notice and condensing notices discussion I was rather skeptical being a European, being a lawyer from -- as to what this might actually lead to, and whether it was really a useful exercise. In the meantime I've become something of an advocate if not a fanatic of condensed and layered notices because I have understood that the educational function of giving information to citizens and consumers is decisive.

And in this respect I must say having heard Amy Friend and Loretta Garrison I'm extremely impressed with the research findings and the work that has been done in the United States in this field.

We have transparency and information qualitative subject as a key element in European data protection law, but we don't have so far, as far as I know as to my knowledge, any comparable research into the effect information is being given to European citizens and consumers, and I'm convinced that there's a lot we can learn from the United States experience.

When we started to draft what was later to be called the Berlin memorandum of 2004 on layers and condensed privacy notices we deliberately chose language which was so general and phrased in such general terms that it was to be applied to the private sector as well as the public sector.

As Marty has said transparency is of key importance, not only on the marketplace but equally in relation between citizens and government. And transparency is also a key element in European and for instance German data protection law. The data subject has to be informed when his or her data are being collected, about the legal basis if there is an obligation to disclose personal data, about the purpose for which the data are being collected, about the identify of the comptroller, the recipients or categories of recipients, and even the existence of a right of access or correction of these personal data.

But so far as I've said we don't really know how well information in the European context is being received and how effective it is.

Certainly information is a prerequisite for choice, you could even say it's a prerequisite for freedom and for an informed choice that can be made about the use of personal data. But if information is too complicated, too complex, to read, too cumbersome, it doesn't fulfill its function. Therefore it is, I think, in the off line as well as

in the on line world of utmost importance to improve in the understandability, readability of any information which is given by governments to their citizens. And in this respect I'm sure that Europe has still a lot ahead to improve practices at hand in European Union member states.

We do have rather complex and very sophisticated data protection rules that much of it is not too well understood by data subjects. There are a lot of certain rights, possibly more rights in relation to private comptrollers as with respect to government comptrollers. But there are rights, but they can only be exercised if data subjects are informed about the existence of these rights.

And the European directive very clearly says informed information is a key prerequisite for all these rights and options citizens should have. I have to indicate at this stage that the European data protection directive, as you probably will know, only applies to the so-called first pillar and the European union structure, which means basically more or less the private sector, but there is now on the table a draft framework decision in the European union which aims at extending data protection rules to the third pillar, meaning the justice and police corporation, therefore here is where government data processing comes into play. The European Union is aiming, this is not the law at this moment, but there are discussions and negotiations in the Council going on to extend the rules laid down in the data protection directive of 1995 to the public sector. And that's where information becomes crucial and understandable information becomes so important vis-à-vis the government -- in the citizen/government relations.

Now processing operations have to be made public according to the European directive in articles 18 to 21. There are certain publicity requirements, but this publicity strangely enough only requires notification vis-à-vis the supervisory authorities. This is a slightly different concept. Obviously the data subject has to be informed if data are collected about him or her, that's the more important side. But at the same time there are certain publicity requirements vis-à-vis the supervisory authorities there.

The structure, and the practice in European countries differs. Countries such as Germany and France have opted to use exemptions from these notification requirements by installing privacy officials within companies, the same applies to the public sector, where other states such as the United Kingdom, Spain, Poland and the Baltic states for instance, have strong notification regimes where you have put up registers, even public registers, of processing operations.

So there is a certain difference in some European countries, but what is more important the European directive requires also risk analysis.

When I talk about risk analysis this means what kind of risks any processing operation might cause to the privacy and transparency rights of data subjects.

Now these risk analysis and prior checking exercises required by the European directive are not themselves to be made public, at least the directive doesn't require this, and it's an interesting question why this should not be made public. I can't see -- even in the government context I can't see in general any convincing argument for keeping these risk analysis secret from the staff, and as more and more European countries, since the beginning of this year even the Federal Republic of Germany have adopted Freedom of Information legislation which applies to the public sector. One can surely ask the question why these risk analysis should not be made public following FOI requests. That is an entirely new field which hasn't been decided as now jurisprudence on this question has yet, but I personally would advise any government agency within my jurisdiction in the State of Berlin to actively make public this information in order to increase transparency and trust even in the government sector.

So I would leave it at that at the moment, but I'm happy to answer any questions in the discussion.

Thank you very much.

(Applause)

MS. LEVIN: Those are very exciting remarks to hear on transparency.

And now we'll shift back to this side of the Atlantic and Eva Kleederman will give us an overview on notices within the federal space, which now will follow with DHS perspective.

MS. KLEEDERMAN: Thank you.

First I want to apologize for coming late. Toby worked so hard on organizing this and creating an order and I truly do apologize.

I'm going to give an overview of the statutory requirements on the federal government for notices and try to convey a sense of how they provide transparency in the sense that we've been talking about.

The Privacy Act of 1974 as most of you know was enacted in response to the excesses of a paranoid administration that secretly collected information about

individuals, about their personal lives, the exercise of the constitutional rights, and other matter not intrinsically related to the operation of government. In reaction Congress sought to promote individual privacy by requiring federal agencies adhere to certain guidelines for transparency and accountability in the collection, use, disclosure and retention of personal data.

Underlying the Privacy Act are five principals known as the fair information principles about which there is always great discussion. These principles require notice when records are maintained about individuals, that is that there should be no secret records. Maintenance of only those records the agency must collect to fulfill a statutory purpose, and use of the records for only the purpose collected, opportunity for record subject to see and correct information maintained about them, assurances that information used is relevant, accurate and up to date and complete, and protection of data against unauthorized loss, alteration or disclosure.

In preparing these principles the Privacy Act requires agencies to publish a description of each system of records the agency maintains, and the Privacy Act actually prescribes the data field, the name and location of the system, the categories of the individual's on whom records are maintained in the system, the categories of records maintained in the system, the authority for, purpose of, and each potential use of the records contained in the system, agency policies and practices regarding storage, retrieveability, access controls, retention and disposal of the records. The title and business address of the agency official responsible for the system of records, the agency procedure for making inquiry about the existence of records pertaining to ones self in the system of records, the agency procedure for affording individuals access to records about themselves in the system of records, and for contesting the contents of any record, and finally the sources of records in the system, that is whether information comes from individuals, complaints, commercial data vendors and the like.

To effect notice to the public these systems of records notices called SORNS must be published in the Federal Register before an agency may collect any information from the individual or from any other source.

Well you asked yourself, what kind of notice is notice in the Federal Register, who actually reads that? Most people don't so Congress provided in the Privacy Act that agencies must, at the time of collection of the information from individuals, inform individuals from whom they are collecting information about the purpose of the collection and the probable uses of the information collected.

This information provided at the point of collection is called the Privacy Act

statement. It's provided right on the form, whether paper form or electronic form used to collect the individual's information, and it's kind of a condensed system of record to notice.

The Privacy Act statement must contain four elements, the legal authority authorizing the request for personal information from individuals, and whether or not it is mandatory that the individual provide the information; must state the purpose for which the information is intended to be used. The Privacy Act statement must also inform the reader of routine uses which may be made of the information. A routine use is a term of art, it is a use of the information that has been publicly announced through publication, again in the Federal Register. And finally a Privacy Act statement must alert the individual to the ramifications of not providing all or any part of the requested information.

A good example for those of you who are familiar with OPM form 71, this is a federal employee leave slip, it states that section 6311 of Title 5 of the U.S. code is the authority for the collection, it informs that the primary use of the information collected is by management and payroll offices to approve and record use of leave. It informs that additional disclosures may be made, for instance to the Department of Labor for Workers' Compensation Administration purposes, to a state unemployment compensation office, et cetera.

It also informs that furnishing the data is voluntary but failure to provide the data may delay or prevent action on the request for leave.

Understanding the sensitivity of the social security number Congress included in the Privacy Act a special requirement for notice, again in the form of a Privacy Act statement when a government entity requests individuals to disclose their social security number. It is not unusual to see a Privacy Act statement with two similarly structured paragraphs, one specifically addressing collection of the social security number and the other addressing collection of all other personal data requested.

This requirement for notice to individuals disclosing your social security number is the only provision of the Privacy Act that applies to state and local government agencies as well as to federal agencies.

Moving on from the Privacy Act, section 208 of the E-Government Act of 2002, this is the privacy section, section 208, reflects Congresses recognition that agencies maintain a great deal of personally identifiable information outside the Privacy Act system of records framework. As you know the Privacy Act notice and safeguard requirements apply when

records or information is retrieved by an individual's name or unique identifier. Congress through the E-Government Act wanted to ensure that agencies provide transparency regarding the handling of identifiable information that's maintained other than by name or identifier. And it did this through the vehicle of the Privacy Impact Assessment.

I won't go into the details of when a Privacy Impact Assessment is required, anybody who is interested can read about that on our website, it's OMB Memorandum 03-22.

But suffice it to say that a Privacy Act statement, if a Privacy Act statement is a condensed system of records notice a Privacy Impact Assessment is an expanded system of records notice. Like a system of records notice a Privacy Impact Assessment, or PIA, must be made available to the public through publication in the Federal Register or posting to the agency's internet site or by furnishing it upon request to an individual.

A Privacy Impact Assessment describes how identifiable information is handled in administering of an agency business process. It provides much of the same information that agency data management practices as the system of records notice. Specifically what information is collected, that is the nature and the source of the information collected, why the information is being collected, what is the purpose, for instance to determine eligibility for a benefit. What is the intended use of the information? For instance it will be used to match against other information to verify existing data. With whom the information will be shared, for instance another agency for a specified programmatic purpose. Whether providing the information is the individuals choice, and what mechanisms if any are provided for consent to particular uses. What administrative and technical controls are used to secure the information. And finally whether the information is or will be maintained in a Privacy Act system of records. That is whether the information will be retrieved by name or unique identifier.

The Privacy Impact Assessment differs from the systems of records notice in that it should have an analytical component, specifically an assessment of what the privacy risks and effects are of administering identifiable information, and what risk mitigating measures or alternative processes were considered or adopted for handling the information or for conducting the business process.

Ideally the PIA should demonstrate to a reader that the agency is engaged in the dynamic process of protecting privacy, as distinct from the systems of records notice which really paints a static picture of how the information -- how the agency maintains information.

Section 208 of the E-Government Act also established in law a measure that OMB had previously articulated requiring agencies to post privacy policies at major points of entry to their public internet site. This practice reflects the principle that visitors to a site should have notice not only of what the agency does with the information that the visitor affirmatively provides through emails or web forms, or in the course of conducting a business transaction with the agency, but also about what electronic data the agency system captures automatically when a visitor links to the site.

Web privacy policies must address the nature, purpose, use and sharing of the information collected, whether disclosing the information is mandatory or voluntary again, and how to provide consent where consent is an option, application of the Privacy Act to information collected, and if the Privacy Act applies, provision of the required Privacy Act statement and a statement of Privacy Act rights, application of any other privacy protecting law, for instance HIPAA or FERPA, and again any statutorily required statement and also a statement of rights under that particular statutory framework.

The nature and use of any electronic information automatically collected, such as the IP address or the location and time of visit for site management purpose for example, appropriate protections when information may be collected from children under 13. The web privacy policy must inform about the children's online Privacy Protection Act and inform parents about how they can provide consent and access to their child's record.

It must inform the reader about the application of any tracking technology, and it must inform the reader about the safeguards and controls applied to security information and to protect its integrity and liability.

The E-Government Act and OMB policy require that web privacy policies be clearly written in plain English, as all the preceding commenters have noted, either at the single notice or in layered format with short highlight notice linked to a full explanation. The web privacy policies should be prominently placed at obvious locations.

And finally the E-Government Act requires that web privacy policies be made machine readable, that is translated into a format that is automatically readable by a browser so that a user can at a glance get a very high level of overview of the agencies information handling practices and determine whether or not they actually want to visit the site.

This machine readable policy affects the principle of choice. The reader then determines whether or not to follow on with the transaction.

There are several other notices, these are the primary ones, and I'll stop here and let my colleague Liz Withnell discuss some particular examples of these kinds of notices.

I think that's what you are intending to do.

MS. WITHNELL: I hope I'm not telling tales out of school, but we did have a conference call ahead of this session to discuss what we were going to talk about, and I thought well my remarks can be really easy because basically we comply.

Everything Eva said, we do.

Basically to react to some of the comments I've heard it seems to me in the government sphere we have layered notices. I'm going to start sort of from back to front.

Privacy Impact Assessments which are the most current and the most recent types of notices that have been mandated by Congress require agencies to in a full manner, or to the extent that agencies are doing this, describe what it is they are doing with personal data.

To me the E-Government Act is basically the Privacy Act brought into the modern age and into the electronic age, and at the Department of Homeland Security we have written guidance to our components to tell them how we think that they should write a Privacy Impact Assessment, and so we have a series of questions that our components are supposed to answer, and then they're supposed to engage in some analysis.

And the point is that before you begin a program, or before you begin a data collection we need you to think about the privacy impacts of what it is you're going to be doing. And we need you to answer the "W" question, who -- now who are you going to collect the information from; why are you going to collect the information; what purposes will you put this information to; who are you going to share the information; what is the statutory basis.

All those questions that really go into making up how you handle personal information in the government sphere. And we ask you to write that in a sort of long discursive way, it is prose, it's not in a box, but you know, we think if they're all consistent people will get used to reading them and so there's a benefit to that.

And we do require them to be finalized them to the extent feasible before you flip the switch on your database and so that we know that you've considered privacy and all the aspects of your activities.

And then we post them on our website and sometimes in the Federal Register to make sure that there's notice.

And I want to give a plug here just for a couple of seconds to the poor old Federal Register. In putting together my remarks I thought I'd do a little research and I probably didn't do enough, but for those of you who don't remember, and this was a long time ago, the Federal Register has been around since 1935. So I sort of feel like in this day and age if we don't read it it's our own fault, it's been there for a long time. And the point of the Federal Register, and the reason that it became part of the law, is because there were times when even the government didn't know what its regulations were and cases were brought and claims were dismissed, or you know, convictions were overturned, et cetera, because nobody knew what the rules were because they hadn't been published.

And so we've had the Federal Register for a long time, and whether it's good, bad or indifferent it is the vehicle by which the government communicates with the public at this point in time.

In addition to Privacy Impact Assessments, which I think of as a sort of a long version of a system notice, agencies are required, as Eva said, to write systems of records notices, and that is a requirement in the Privacy Act. And the Privacy Act does tell you what information goes into a system of records notice, and there are nine categories, not seven, which some of the other folks have talked about, you know, consumers can only deal with seven sort of sub-sets of information, but we are required to include nine. And it seems to me the categories make sense. I mean the one thing I like about the Privacy Act, which is, you know, the poor Privacy Act gets kicked around a lot because pay it's, you know, old and needs to be refined, et cetera. I kind of feel that Congress was prescient in a way and wrote a statute that was good for the ages. It may not be good in all its respects, but in telling people the kinds of information we're collecting through the vehicle of a system of records to me makes a whole lot of sense.

The Federal Register has a drafting -- a document drafting handbook so we're not writing these notices based only on what's in the statutory language and the categories. And the drafting handbook in addition to telling you things like what the margins are supposed to be on your notice, and for those of you who care it's an inch on the top, and an inch on the bottom, and an inch on the right-hand side, but an inch-and-a-half on the left-hand side, because you know, back in the days when we stapled those things, or punched holes in them we didn't want to obliterate any of the words, so it's an inch-and-a-half on the left-hand side.

But in addition to telling us, you know, sort of the mechanics of how to write a notice there is a whole section in the drafting guidelines, and if not there then certainly on their website, on how to write these things in plain language. And if you read it, you know, it will hark back to eighth grade grammar. Write in the active voice, write short declarative sentences, don't use split infinitives -- in case anybody remembers what those are at this point in time. And the one thing that they did say that sort of bothered me because I tend to use a lot of synonyms is don't use synonyms, you know, for the same term because it confuses the public. If you're talking about cars keep talking about cars, not automobiles or vehicles. So there are some rules in there that are peculiar to drafting style for the federal government.

In addition to that, and for those of you who may recall, there was once upon a time, I think back in the late '90s, an Executive Order on writing in plain language that was issued by President Clinton. And not only is there this Executive Order that says thou shalt write in plain language short declarative sentences, short paragraphs, et cetera, et cetera, but there's also a government website, little did I know, www.plainlanguage.gov, that seriously, you know, goes through the same kind of scenarios, gives you the same rules, gives you some examples of things not to say. And so the -- my point is that the tools are there for folks who are writing system notices, Privacy Impact Assessments, whatever we have to do in terms of regulations, the tools are there for us to make these notices not only transparent but understandable to the folks who we hope will be reading them.

The final part of sort of the layered notice is at the back end is the notice that the individual receives when he or she is asked to give information in an information collection. And that can be either electronically or in a paper form.

I know most of us here, Eva mentioned the Privacy Act notice on the leave request. You know, once upon a time in one of my offices we sort of whipped that off before we even gave it to you because we assumed everybody had already read it, and then we thought oh, no, no, no, we can't do that because you're supposed to have notice. Some of them are written sort of strangely, you are required to give the statutory basis and most people don't care, particularly in the public. I mean they're not going to run to the U.S. code probably and look the stuff up. But you are required to give the statutory basis.

You are required to summarize your routine uses, and it is a term of art what a routine use means, but the more you read about these things and the more you see in these notices what the government is going with your information the better informed you become. And there is an art to writing them in the sense that they can be written in sort of plain language way to convey the essence of what it is we're collecting and why.

And we can do it in a paper form and we can do it electronically, and also on our websites when we do this electronically there are privacy policies that are there, and I think these days, if I'm not mistaken, more and more consumers are aware of at least looking at the privacy policy on a website in terms of collection.

At the Department of Homeland Security we take privacy seriously because we have the first statutorily mandated privacy officer, and one of her roles is to ensure compliance with the Privacy Act, and the other is to make sure that we're all writing Privacy Impact Assessments, and sort of overall we're to guide privacy policy for the Department.

We comply with all the things that Eva has talked about, and all the notices that I've mentioned, and all the layering terms of notices, and we try to the extent that we can to make sure that what we're producing and publishing in the Federal Register and elsewhere is comprehensible as well as comprehensive for the public.

I mean one of the things that we do in our office since we approve all systems of records notices before they are published is make sure the routine uses make sense for the system that you're creating, that you are transparent about the categories of individuals and records, that you've thought about what it is you're collecting and why, and what you're going to do with it, and it's accurately reflected in your notices, and also in your PIA.

Thank you very much.

(Applause.)

MS. LEVIN: And then sort of the bookend to the panel will be Paula Bruening talking about the perspective of the public and civil society.

MS. BRUENING: Thank you, Toby, and thank you for inviting me to be here today, I'm happy to talk about this issue.

And I think every one of us at one point in our discussion has taken some kind of look back into history are going over a death note in 1935. I'll just take you back to 1996.

When I was at the Commerce Department and we were in the first phases of encouraging the public sector to post privacy notices to adopt privacy policies so that the public could be more informed about what companies were doing with data and data collection, and the underlying premise of that exercise and that effort was to provide

consumers with more choice, to give them more information about the companies they were dealing with in the online world so that they could decide whether or not on the basis of their privacy policies, as well as other things about the company, they wanted to go ahead and do business with them and turn over information.

And it's a very fundamentally American way of approaching these things. We sort of base so much of what we do in this country on our ability to choose and to make individual decisions.

A European friend of mine went into the grocery store looking for toothpaste and came back and said Paula, you Americans make things so hard for yourselves, you have 15 kinds of toothpaste to choose from, and as someone who doesn't know the brands I have to figure out which one I want to use.

But whether it's good or bad it is the way we've done things in the United States for a very long time, and it's the way we sort of define ourselves, and therefore the way our starting point I think in the late 1990s during the internet boom about, you know, how we were going to make decisions about our personal information.

I think that that is fundamental, but I think in the ten years that have gone since then we've learned other things about privacy notices and privacy policies and what their function is. And while choice is still critical to all of that we've also learned that requiring and encouraging companies to post privacy notices provides a real discipline around information practices. It really forces them to do privacy housekeeping, to really look at their systems, look at their collection policies, and ask hard questions about what they're doing, why they're doing it, whether they actually need to have the information that they're asking for or whether it's perhaps being swept up as a result of some technical decisions that were made in creating software business models.

And it also I think encouraged them to make meaningful decisions about what it was that they really needed and wanted to collect. And perhaps encouraged a more surgical approach to information collection, which I think it was important to sort of principles of data minimalization, whether they were stated or not I think that companies if they were required to disclose what information they were collecting perhaps would make choices not to collect quite as much or not to collect information that they didn't fundamentally need because it would not reflect well upon them and their data practices.

So overall what this really did was in addition to providing transparency to further choice it also provided transparency across the board about what we were doing in the commercial space of that information collection. And it provided that information to

individual consumers, yes, but also it provided that information to government and it provided that information to advocates, and to media, all of whom were providing pressure on businesses to do the right thing, to be responsible about their information collection and their data practices.

So what we, you know, really pushed hard in that space and found that they had those benefits I think it's important that those benefits also be available to people who live in the United States, not just as consumers but as citizens, and that that kind of transparency is as important in the government space as it is in the commercial space. Especially in instances in government collection of information the citizens may not have as much choice about whether or not they turn over information than they might when they're going to a company online or in the store.

For me to engage in certain government activities to avail myself of government services I may not be able to choose quite so much about what kind of information I turn over.

And so that transparency and that ability to see what it is the government is doing, what it is that they think is necessary for them to have, how they plan to share that information is perhaps even more important. It does provide us with more information for advocates and for media, and for citizens, to see what it is the government plans to do and gives us the opportunity react to that not only in real time as we're engaging in our individual transaction or interaction with government, but also in the wider public policy arena where media and advocates can, and government oversight, can also take a look at what's going on in individual agencies so that decisions can be made in a wider public policy debate about what's appropriate.

And I think it goes without saying that this is particularly important right now when the appetite for data is so keen in government, and when I think we feel as a society more sensitive to information collection and use by government than perhaps we have in other times.

I'd also like to comment that there is no question that providing these notices is a challenging -- it's a real challenge, and I commend the work that's going on here. I've been following Marty's work since it began and we did convene a consultation at the Center for Democracy and Technology on privacy notices where we brought together government and advocates and businesses to talk about some of these challenges and to talk about what it is that consumers are looking for, what it is that they really need, what communicates well. And I think that from an advocate's perspective there was the sense that notices had to get better. To be useful they had to work better than they were

working at the time.

I think our concern was that whatever templates were produced to the extent that we might actually issue requirements, government issued requirements, about notices. They had to be based on very strong well-constructed research, and so we're pleased that that work has gone forward, and I'm going to be interested in digging further into the results of the research that came out last week.

But I think the one thing that going forward, since we've sort of looked at this historically, what I think is also very important to bear in mind whether we are in government or in business is that the way in which we're going to receive content, the way we're going to interact with businesses, and the way we're going to interact with government is going to happen on a very wide range of platforms, and through a wide range of mediums. It may be through the old-fashioned paper and a number two red pencil, but we may be getting information through our telephones, through our PDAs and through devices that we may not even have any imagination for right now.

I'm currently working on a project on radio frequency identification technology, and trying to apply principles of fair information practices when that kind of device is used in the commercial space.

I cannot think of a place where it's more challenging to provide notice than when you are talking about data collection using these tiny, tiny microchips that you really -- the average person can't see if they're not looking for them.

And so I would say that this kind of effort in making these notices better and more effective is one that's going to have to be ongoing, and that we're going to have to keep -- because we're going to keep bumping up against new technological challenges to the way that we craft these and make them useful to our consumers and citizens.

Thank you.

(Applause)

MS. LEVIN: Well let's begin our discussion as a panel with sort of I think the overall key question which is what have we learned from the research, from the experience in the private sector that you think is applicable to the government space.

You started your work in research I guess 2001, we're now into 2006. I would like the impact of what has been learned to be sort of telescoped much more

quickly into the government space, so let's jump on the idea of what would you then transfer to the government space in your work, and maybe I'll start with the government.

MS. GARRISON: I guess the first thing that I think is most important after listening to all these wonderful presentations today is know your audience, know to whom this notice is being addressed.

We actually have different audiences here for a lot of these notices. For example what Eva was talking about and Liz was talking about, well primarily Eva, a lot of this is for the government to comply with federal mandates to identify certain information and it has to follow a very prescribed statutory pattern. This is great for people like Amy and me because we're regulators and we get paid to read this stuff.

But for most of us normal people this goes right out over our heads and out the window, actually it goes right into the trash because it doesn't mean anything to us, it's all gobbledegook. We frankly are very, very busy people, we just don't have time to read this sort of stuff and delve into it deeply.

So I think that's the most important thing, and that's really what Amy and I have learned, and our colleagues at the other agencies, have learned from this very intensive consumer research. Because what we thought were wonderful notices, they were simple, they were clear, they were done with short bolded bullet forms, in fact all bombed because they just simply didn't work.

Just another quick comment about the word "choice" which has been used around the table here and it's another thing that we learned in our research. As Paula said, we do as consumers expect to have choice, and of course we talked among ourselves about the notice providing choice for consumers. But what we learned is that choice can be -- can in fact be counter productive in certain context. For example, in Gramm, Leach, Bliley with your financial privacy notices a company can share very broadly, and under federal law then is required to give you an opt out notice to give you choice about whether you would want to limit certain sharing.

But there are other companies that will in fact share in a very limited way. For example, they may only do it for what we call their everyday business purposes and for their own marketing. And they're not required to give any opt out notice and they may not give an opt out notice. Now there is no choice for the consumer in that sense, but yet that company may be sharing in a minimal way which a lot of people would really prefer. The problem we found when we phrased the notice in terms of your choice to limit our sharing is that consumers looked for that choice. So in the interest of keeping it neutral

and balanced and objective we actually reframed it to say that the company that chooses the way in which it shares, and in certain circumstances you, the consumer, have the right to limit the information.

So again when you get down to this level with consumer testing very often things that make sense to you, things that think are really fundamental, in fact may not play out that way when you do actual consumer testing.

MS. LEVIN: Amy?

MS.FRIEND: Sure. Just to sort of second what Loretta said is that we were continuously surprised by what things worked and what didn't.

We, under the privacy regs we said companies could say if they did sort of routine sharing to process transactions or share with credit bureaus or give to their regulators, they could say we share as permitted by law, and that never worked.

So then we said well they share for their everyday business purposes, and people said well, what's that? And they were so suspicious.

Well, then they share for their normal business purposes. Normal business purposes, does that mean they can share for everything?

So we ended up having to go -- I guess it was routine and normal, we ended up with everyday business purposes with a little explanation up front that said all companies have to share for certain reasons in order to give you what you're asking for, in order to remain in business. And so that coupled with everyday business purposes worked, but we never could have imagined that when we were sitting around and drafting.

So it's sort of expect the unexpected. And consumers really do steer you in the right direction.

The other point is that design really matters. You know, what we found was that this tabular format made a huge difference. So as plain as the language was that we were using it made a difference whether it was presented as prose, or in a table.

When we drafted the privacy regulations we thought that we were quite progressive because we had taken some of the existing working government, particularly the FTC, in requiring plain language use drafting privacy notices. We talked about white space, about bullets, about, you know, not using legalese, and we ended up with the

privacy notices that you see today.

So we needed a directive that went beyond just plain language.

The final point is that -- and this we really will have to test in this second phase, is standardization. It seemed to us the trend was that having this standardized table, a standardized presentation really made a difference.

Again I think about the nutrition label and how people know where the table is, what the table says, and how to use it, and if they care about fat they know exactly where to look, if they care about sodium they know it's there. So it's that sort of standardization that really allows for greater usage and understanding.

MS. LEVIN: Marty?

MR. ABRAMS: A word of caution. I think the research is fantastic, and I think that the research -- the continued quantitative research is also well, but I would remind the folks in the audience that these privacy notices are not static, that typically in the private sector organizations revise their notices every year, every 16 to 18 months, and that's there's an ongoing process of saying how are you using information, how do we then have to reflect that in our own internal policies, how do we then reflect that in the internal policies as we present it to the outside world, and what does that mean in terms of a consumer notice.

So my point is this: that since this is not static. And since we know that you can incrementally improve notices today I think there should be a desire to begin today and say, let's improve the notices, let's learn from what has been done by others in the private sector and in government to improve notices with the intent that as we go through multiple cycles of revision of our own internal notices that we will get to the point where we have the research that creates the gold standard, then leads to the process going forward.

I would be very disappointed in the period of time when we are collecting a great deal of information, both directly from consumers and from third parties about consumers, if we didn't improve our notices today so people have something that is easy to understand and comparable.

So that I think that the goal should be better notices this summer, and I'm honestly saying better notices this summer, rather than just better notices in five years.

MS. LEVIN: Paula?

MS. BRUENING: Well I think that I would concur with the concern that there be a standardization and comparability so that there is that ability to compare across agencies, across collection practices. But I think that it's also going to be really important to say that that doesn't obviate the need for the more comprehensive notice that really lays out in detail what that agency's information practices are. That if you want to still have the optimal transparency we have to be very careful that in the attempt to be efficient and to communicate clearly and simply and well then we haven't, you know, purposefully or inadvertently hidden other information that should really be out there and be made public whether it's something the consumer himself or herself reads, but that it is out there and that it is available to the citizenry at large.

MS. LEVIN: Well, let me ask you, do we need different notices for the legal policy community than we need for the general public, or should there just be one notice? Should it be the same?

MR. ABRAMS: I believe that you have to layer notices. I believe that it's important to have an external statement that defines in detail how the privacy information is collected and the purposes for which it's going to be used, because that really defines and limits the purposes and I think that's important. I think that others, at least in my world, would share that view.

I think that it's also my view that notice that is so attractive because it is detailed and because it begins to give us all of the important things it is to understand the total picture, that's not a notice that an incredibly busy individual can deal with.

If I'm at an airport, okay, and my information is being shared with the Department of Homeland Security, which it is, I would like to know the type of information and the general purpose and what I should do if I'm harmed by that conveyance of information.

So I think it's very important to have a notice that is a tear sheet that gives the general picture, that gives me a sense of what is collected, what it's used for, and what the options are.

MS. LEVIN: Any other comments?

MS. FRIEND: Well I would say in the notice that we put together we did address all of the elements that are required now by the Gramm, Leach, Bliley Act, and by the Fair Credit Reporting Act. So the Fair Credit Reporting Act goes to certain affiliate sharing

and opt out opportunities, and the Gramm, Leach, Bliley Act says you need to talk about what information you're collecting, what information you're sharing, with whom you may be sharing. We've interpreted by general category. Actually the statute says, how that information is safeguarded, what do you do with information about former customers, whether there's an opt out opportunity, and what that may be.

And we looked at taking some highlights of that. What we found was that consumers were able to work with less information but they were also able to work with more information, and that when we provided all the information in the format in which we did it worked quite well.

I think we did go slightly beyond what federal law requires in a few ways. One is we say why are you getting this notice, which federal law doesn't require, and what we found is that consumers liked knowing that federal law required this. So this was a document that their institution needed to give them.

So contact information is also something that's not required by federal law, so that went beyond.

But when I think about a document that would be more complex than the one that we developed I'm not sure it imparts any more information at all. A lot of the privacy notices now are just complicated because of the wording. They also put in some additional information they think consumers might want to know about identify theft and things like that. I don't think we've reached any position at all about whether that's okay or not.

So providing a more complicated document that goes beyond what we've developed I'm not sure it gets anywhere, or even provides more accountability for that institution.

MS. LEVIN: In the government space frankly the notice writers are lawyers. There are many of them I think here in the office, in the auditorium today. Lawyers have the strong hand in writing our systems of record notice, our Privacy Impact Assessment.

Should that be the case, should it be more collaborative? What about the actual preparation of these notices? How would you recommend we do that?

MS. WITHNELL: Toby, I think it's fair to say that in most agencies there is a collaboration between the program people who know what the data is and the lawyers who are worried that they're not expressing themselves accurately or, you know, or

complying with the law.

So I think you can't sort of generalize to say that it's only lawyers writing these notices. I mean my colleagues in the privacy world are I think by and large mostly non lawyers, and that may be a good thing in terms of their writing ability.

I think that our notices are constrained to a significant extent by the requirements of the statute, and that we do have layered notices as I mentioned, and you know, the one that the individual will get, if not at the airport then when he makes his plane reservation, will be slightly different I think than the notice that he will get if he goes on a website and reads a Privacy Impact Assessment about that particular collection, or goes to the Federal Register and reads in some detail the systems of records notice.

And so, you know, perhaps what we need in the government sphere is sort of the education piece that says to folks, go read this stuff. Because it's not like we're not writing this, and it's not like we don't have the tools out there that say write it plainly, clearly, you know, make it understood, et cetera, it's just we need to get sort of the horse to the water.

MS. LEVIN: Any other comments on this?

MS. KLEEDERMAN: I think I concur with what Liz says, but I think I would also note that the Privacy Impact Assessment, the more discursive notices, are necessarily written by a combination of people, not necessarily the lawyers; in fact probably not the lawyers, probably the system owners, IT security people, possibly the lawyers just to make sure all the "Ts" are crossed and "Is" dotted. But the more discursive notices definitely need to be a coordinated effort.

And perhaps then it might be the lawyers responsibility to make it clear and plain English after that to make sure that it is understandable by the lay person.

MS. LEVIN: I don't really mean to encourage the employment of communication writers across the government but I'm wondering if in terms of the research that you've done to what extent were the communication experts in the project important?

MS. GARRISON: Well they were vital. We couldn't have done it without them. I mean you can go back to 2001 when we wrote our sample clauses the very first time and companies used them. Starting from there it was, you know, these were trashed.

When we first put our privacy policy together for the first round of testing we actually adapted a couple of those that were included in the ANPR that we published as

examples of possible approaches. Two of those were drafted by agencies, one of them in fact was drafted by several of the Chief Councils. They thought they wrote a spectacularly clear and easy to use notice. Well, it completely bombed.

When we tried to put our first notice together after testing with consumers and getting their preferences on various components that one bombed as well.

So it wasn't until we started working with our researcher who basically kept telling us that we've got to let go for the lawyers, we can't be as absolutely precise as we were trained to be, that we need to let go a little bit so that in doing so consumers in fact would be better able to understand what we were trying to tell them.

MS. LEVIN: Are there some inherent differences though between the public and private sector notices that make transparency different in the two sectors? And I think we sort of talked about particularly systems of record notices which many of you have seen. Is that inherently a different kind of document than the notice you might get at an airport?

MR. ABRAMS: I believe communication is communication. And, you know, I believe that individual actions drive behavior, and I believe that individual actions in the private sector drive the way companies over time use information to create value for themselves and for the individuals they serve. And I think the same thing is in play in government.

You know, I understand the limitations related to the Privacy Act and the E-Government Act I understand, but I would also say that when I began working with general counsels of multiple companies they said almost exactly the same thing about the importance of precise language in notices. Dale Skivington, who I think is a really fantastic individual, is a lawyer at Eastman Kodak Company, and she took over as Chief Privacy Officer and when she did so their online notice was a page long. She took a look at unfair and deceptive practices actions by the Federal Trade Commission and decided my God, our notice needs to protect us, and pretty soon it was seven pages long. And it was that seven page notice that convinced her that Kodak had to be part of the project.

When she was confronted with HIPAA with it's 31 required elements for them to give a HIPAA notice to their employees her HR people said well why don't you play around with this multi-layered notice concept in developing because it was cited in the preamble to HIPAA regs. And she developed it and she was reluctant to use it because by taking it down to the box she made it easy to understand what was going to happen with the information but it wasn't precisely mapped to the 31 elements.

She was told in no uncertain terms we're going to use this because it is just so much better in communicating with our employees, communicating the issues is more important than being precise.

I think that the advice from the communications expert just let go and find a way to communicate innovatively while still understanding the importance of compliance is absolutely essential.

Now I say that as an anthropologist and as a non lawyer.

MS. LEVIN: I'm ready to see the design for the top layer of the SORNS. We'll start taking bids for design suggestions.

All right, I'd like –

MS. KLEEDERMAN: This may be heresy but I'm not sure that the SORN really is all that difficult to understand. It's broken up into categories, the data fields are bolded, and except for perhaps the word routine use there are no terms of art that are particularly arcane. It may be that the print is too small and it's too difficult to find, and that's not to say it couldn't be improved and I think agencies are working on writing things in easier to read fashion.

MS. LEVIN: No, my suggestion is -- I actually agree with you, I think the headings are all there, but maybe for the individuals who don't want to read however long the SORNS are you just have something on the very top that is basically sort of a quick, maybe it's even tabular, that very quickly gives you some of the highlights, so for those people who just want to have a general sense quickly that they would get it. Sort of a nutshell as an idea.

Okay, let's see now if there's some questions -- if you'd line up behind the mike, and if you'd be so kind as to just introduce yourselves, your name and any affiliation if one applies, so that we have it for the transcript.

Thanks very much.

MR. SCHNEIDERMAN: Good morning, and thank you for this very valuable session.

I'm Ben Schneiderman from the University of Maryland, Human Computer and Interaction Lab. I'm delighted and very pleased to hear about the empirical research that

was described with 66 consumers that was attempting to understand the principles.

And I hope that you're going to take this forward to develop a set of guidelines of best management practices that translate to ways of doing it, not just the research.

I might cite to you the National Institute of Standards Common Industry Format for Reporting on Usability Testing, which I think is the right methodology. I think your expansion to 2000 users is just the right direction.

My question is to the DHS participants. I was concerned because I heard your descriptions of confidence that you've adhered to legal principles, but I heard no description, and I'd like to hear about your intentions of conducting empirical assessments with consumers on the scale that was described because as the study participants described they were continuously surprised, and I think that's really the essential issue.

So where are we going with empirical tests for the process of whether consumers can understand the current notices?

MS. WITHNELL: Well I think with Toby in the office as the senior advisor for privacy we're definitely going in the direction of consumer research. Quite frankly I'm not sure at this point we have particular plans to go out and conduct the same kinds of consumer research, and I think I would probably look to OMB to a certain extent to see if this could be done government wide.

I'm still not convinced given sort of the statutory and legal requirements and the fact that we do have notices in various venues and of various types that the issue is doing consumer research, but more education. I mean I feel like at this point perhaps from the government side what we need to focus on is getting people to read what we've written, and getting some feedback as to whether or not what we've written makes sense to them.

And there is a mechanism if you use the Federal Register to make comments on system notices, and I have noticed, with glee actually, that people are now doing that more and more frequently. So that tells me that, you know, someone out there is reading them.

And there is a way to make comments on Privacy Impact Assessments that are published as well. And so I would hope that that would continue and that we would do more in terms of education, and this seminar is one way in which we hope to educate, if not consumers then the rest of the folks, to sort of bring this message back.

MR. SCHNEIDERMAN: I think it still needs to validate that the education was successful. Unless you're assessing performance you don't know whether it's working or not.

MS. WITHNELL: Well I'll take that back to the Privacy Officer and we'll talk about it.

MS. LEVIN: Thank you very much.

MR. VONBREICHENSUCHARDT: Good morning. I'm Dane VonBreichensuchardt with the U. S. Bill of Rights Foundation. And today I'm the poor stepchild question. This one -- I'm amazed how much work you folks have to go through just to get out a privacy notice. I'm duly impressed. That's a lot of work.

And it is amazing. You think you've got something where everybody understands it and you come up later that nobody gets it at all and you got to go back to the drawing board.

But my question goes to a much more nuts and bolts concern that affects citizens every day on the street. What my privacy notice problem is, my transparency problem is, just to give you a few of them. The Federal Trade Commission, DOJ, Treasury, State, EPA, FAA, GSA, GAO, IRS, SEC, all of them that if you have -- and others, this is just a few that I've directly been involved with. If you have an appointment to go into one of those buildings they say that they require personal identifiable information. They want your name, your date of birth, and in some cases they want your social security number.

MS. GARRISON: Not with the FTC.

MR. VONBREICHENSUCHARDT: Okay. Well actually -- I don't know why but I had that experience, I wouldn't have written it down.

Anyway, the question that I have about transparency is that I realize that that might be a minimal set of records, I don't know how long they keep it or what they do with it, but they will not answer those questions, they will not give you a 7B notice. In fact when you try to tell them that it's in the Privacy Act that they're supposed to -- if they're going to asked for that information what is their authority for asking for it, and what are they going to do with it, and who they're going to share it with, and all of the questions that you folks were talking about.
And if you don't give it to them they won't let you in the building.

And I've made challenges on these things, and in one instance the only break through I had was over at the Department of Justice, and it was a meeting they invited me to having to do with cyber crime, and when I complained about giving up my social security number and my address and my name and all they wrote me back and said well, we checked the records and you are right, there is no requirement, there is no law, it was just a policy. And if you want to, come on, we'll let you in.

Well when I went down there they wouldn't let me in.

So all I'm trying to -- and the reason I'm bringing it up here at this meeting, I'm not picking, is that they all hint that it's Homeland Security's requirement, but not to this date has a single person told me what the authority is for them asking for that, why I even have to show a driver's license to get in this building. I cannot find the law. Now they give me reasons, they'll say well, you know, since 9/11 -- I mean those might be policy reasons but I cannot find anywhere the authority for it, and I certainly have never been notified of those required standards about letting me know whether it's mandatory, voluntary, what is going to occur with that, how long they going to keep those records, who they're going to share them with, what they're even going to use it for.

So I was -- I've rambled on, but that is generally my question, and I suppose the most anchoring question is that what do I do, where do I go? I've filed four years, I never hear back from them. Nobody will respond to me, they just stonewall you, I can't even get the lady from DOJ to even answer my emails or phone calls.

MS. LEVIN: Well I think actually the practices vary from building to building depending on the contractor, and I think we can give you some examples of that.

MS. GARRISON: Well the only thing I can say from inquiries that we've had, and the FTC does not ask for a date of birth, social security number. They ask you to show a photo ID but they do not write anything down, and then you simply sign in.

Now my understanding is that GSA manages the buildings, and that the Federal Protective Service in fact are the guards that are hired to implement the security procedures. So at least for us the agency itself does not have anything to do with those requirements, those are GSA driven because GSA manages the building and therefore access to it.

MR. VONBREICHENSUCHARDT: Isn't that the tail wagging the dog? I mean it would seem like to me that if a security service is under your employ they have to follow

the orders you give them.

MS. GARRISON: They are hired by GSA and GSA is the agency that manages the government buildings, so that the individual agency in fact is not a party to that transaction.

MR. VONBREICHENSUCHARDT: Is that where I go then, to GSA and ask them for a 7B notice?

MS. GARRISON: My understanding -- I believe that would be correct.

MS. KLEEDERMAN: If I might just add, I think that this problem may be remedied when agencies finally implement the HSPD12 because there will be several privacy notices at the point where a visitor enters a building articulating the uses of the information collected.

VOICE: I'm glad to see you're here Mr. Dix as I'm sure you're finding many of Homeland Security's policies are best in the original German.

But actually I want to talk to you, or ask, actually this question is for Mr. Dix, what I'm hearing quite a lot about is dotting "Is" crossing "Ts" and dangling participles –

MS. LEVIN: Could you identify yourself?

MR. SCANAL: Sure, my name is Bill Scanal and I'm with the identity project. My apologies.

I hear talking about margins and gerunds and dangling participles whereas I think the real problem is truth and honesty. We see privacy notices and citizens, not consumers, citizens expect that they're getting privacy when in reality they're getting weasel-worded documents that are privacy stripping documents. This nation, as I'm sure everyone is well aware, has the worst data protection laws in the western world.

And Mr. Dix, I thought that you might want to address what you in Germany, having some of the strictest data protection laws, do when government agencies violate your laws. That it isn't a matter of a slap on the wrist and off for three days of privacy school as the Department of Homeland Security has so often done when they've broken their own privacy regulations.

MR. DIX: Well listening to the gentleman speaking earlier I was tempted to say

that in fact this shows, with due respect for our U.S. hosts, the need for some kind of independent watchdog in terms of -- as a privacy commissioner, which still is missing in this country. You know, that there is a big debate going on between Europe and the United States about the adequacy of data protection standards in this country. Some of these discussions have been resolved, some are still going on, some certainly I'm sure are ahead.

But I would still reiterate what I said, there may be certain aspects where Europeans tend to say we have the stronger protections for privacy compared with the United States, but on the other hand there are aspects and layers and understandable notices, and one of these -- part of these aspects where Europeans can in fact learn from Americans.

So there is an ongoing dialogue across the Atlantic. It's not a one way dialogue, it's goes both sides, but there are certain examples and some have been cited earlier where certainly we would wish from the European side that an independent privacy commissioner would be installed in this country.

MR. ABRAMS: The one point that I think you might have lost in the discussion this morning is when you make notices shorter, when you begin to bullet those notices, when you begin to reduce them to the essential elements there's no room in the document for the weasel words that you mentioned before.

You lose phrases like, you know, we care about your privacy, you lose those phrases from the document and what we have learned in our research, in our focus group research, and I think this came out in the other research, is that consumers don't trust those statements anyway.

So that one of the advantages to the weasel word document -- excuse me, one of the advantages of the short notices is you get rid of the words that you object to.

MS. LEVIN: One more question.

MR. MILLS: Yes, my name is -- excuse my voice I was screaming at the screen, rooting on the University of Maryland -- and also I coach a 15 and under AA basketball team and we have a big tournament coming up.

So my name is Raymond Mills. I'm currently a Communications Director at the DHS, Office of the Citizenship and Immigration Service.

I've worked in the federal government for over 20 years for the Air Force, the VA, IRS, Treasury, and now with DHS. One of the things that I have great hope for is this panel coming together. One thing we haven't had, and I've been involved in data collection from the analysis side, from the communicator's side, and also from the legal side of it. And you really need all three to come together to come up with anything that's going to be understandable and workable for our customers as well as for ourselves.

And the other thing that I'd like to commend the panel on is it seems like we're moving closer to a concept of a generalized process, focusing on the process so everybody knows the steps you have to go through. From there you can customize it and do your communications and come up with the statements that will best serve you and your constituency.

Now my selfish question. As we move into this area of, I guess Privacy Act and what we're going to do online, things like that, I'm concerned with what we are doing, is there going to be a distinguishing procedures between citizens and non citizens?

The reason I'm asking this is because of being in Citizenship and Immigration Services, the ombudsman sort of overviews what's going on. We take problems in from all the constituents that are having some sort of issue with getting their immigration benefits and services. Some of those are citizens, some are non citizens.

How do we handle that disparity? Is there something that we should be planning for, especially if the guest worker program comes along, immigration reform coming along, will there be a differentiation between that data that is captured for non citizens as opposed for citizens?

MS. LEVIN: I think you've covered a wide spectrum of issues. I think in terms of the notice area I think as a policy matter we would want to give notice to any individual from whom we're collecting the information as a policy matter.

Certainly under the Privacy Act there are some very specific constituencies.

MS. KLEEDERMAN: I don't want to get too technical, but if information from citizens and non citizens is being collected in the same system for the same purpose you've got a co-mingled database then you would have a system of records notice and afford at least that kind of transparency.

And perhaps some of the indicia of Privacy Act rights, but just including non citizens in the system of records notice doesn't necessarily afford them all the legal rights

under the Privacy Act. That's a separate issue from programmatic rights, what we're going to be doing on guest worker programs and what systems will be stirred up right now -- I shouldn't say right now, the Privacy Act only covers -- applies to citizens and legal permanent residents.

I don't know whether or not that's going to change. But in terms of administering the notice requirements notice will probably be given universally, the other indicia of Privacy Act rights –

MR. MILLS: Yes, we're preparing a package right now that we're going to vet through DHS Privacy and Council as well that's trying to cover those aspects, so I was just trying to get a leg up on that so maybe I can do that language in there.

MS. LEVIN: Well you're likely to hear from the DHS Privacy Office that we would urge that certainly from the notice, the notice elements, that that transparency be afforded to everyone, and not distinguish.

But I'm very glad to hear about communication expertise within the Department. It's a huge Department and frankly we haven't tapped the communication expertise as yet from our office, and as I think Liz mentioned you're likely to hear from us. This is the initial panel on a very important area. I think going forward we're planting seeds and we hope to do more in the notice area and do better and better notices.

I certainly wouldn't want to stand before you and say that all of our notices have been perfect, that, you know, we know how to do them absolutely perfectly. I think Marty's point is that we want to get better and better as quickly as possible, and I think this panel is a first step really in our effort to do that, to get better and better.

MR. MILLS: Thank you, and I hope I have a voice when you do.

MS. LEVIN: I want to thank our panel today, and all of you. I hope you go home with ideas about how to do your notices better, and we'll look forward to reaching out to many of you in the future to work with us on this effort.

Thank you.

(Applause)