The Privacy Office
Department of Homeland Security
Privacy Office Workshop Series
Operationalizing Privacy: Compliance Frameworks & Privacy Impact Assessments
June 15, 2006

OFFICIAL WORKSHOP TRANSCRIPT

GSA Regional Headquarters
Auditorium
7th & D Street, SW
Washington, DC 20024

PANEL I
OPERATIONALIZING PRIVACY

Moderator:

Toby Molgrom Levin

Panelists:
Jane Horvath
Zoe Strickland
Harriet P. Pearson
Maya A. Bernstein

MS. LEVIN: Good morning. It's my pleasure to moderate our panel this morning. My name is Toby Levin. I'm a Senior Advisor in the DHS Privacy Office. I was quite moved by Assistant Secretary Hawley's remarks talking about privacy as the foundation of programs. That was excellent.

Our focus of this panel is operationalizing privacy. We'll focus on how do we move from privacy as a value, a policy, and even a statutory mandate to making an integral part of our day to day operations, in effect how do we move from privacy on paper to privacy in practice.

I'm particularly honored to be here with four of my, I'd like to say colleagues, in the privacy arena. Generally I would refer you to your bios for details, but I'm going to just give you a little background on each of them because we are honored to have four of the leading privacy officials in the private and public sector today and I want you to appreciate that before we begin.

To my left, Jane Horvath is the Chief Privacy and Civil Liberties Officer of the Department of Justice. She took on these responsibilities in February of this year and the details of the responsibilities are in her bio. Prior to her appointment at DOJ, she served in the private sector in several capacities, including director of the Washington office of a U.K.-based privacy consulting firm and as assistant general counsel of America Online and as associate at Hogan and Hartson.

Zoe Strickland was the first Chief Privacy Officer for the U.S. Postal Service in 2000. She participates in several privacy executive boards and committees, including serving on the board of directors of the International Association of Privacy Professionals, or IAPP, co- chaired the Privacy and Security Subcommittee of the Council for Excellence in Government, and the privacy leadership group of the Privacy in American Business. She's truly become a role model for CPO's in both the public and private sector.

Harriet Pearson is the Vice President of Corporate Affairs and Chief Privacy Officer of IBM. She has served also on boards of privacy organizations, including the IAPP and TrustE, which is a self-regulatory private seal program, and is a member of the Conference Board's Council of Chief Privacy Officers. In June of 2001 she was awarded the Working Woman's first-ever Women Elevating Science and Technology Award, and I'm sure that's in part because of the fact she's both an attorney and an engineer.

Maya Bernstein is the privacy advocate for the Department of Health and Human Services. She began her responsibilities in February of 2005. Maya's involved in a wide variety of matters at HHS, including electronic health records, genetic discrimination, family and child welfare, drug abuse, mental health records, prescription drug surveillance, research on human subjects, counterterrorism, emergency preparedness, and personnel security, as well as privacy.

Maya began her federal career at OMB, where she was responsible for oversight of the Privacy Act. She later served as privacy advocate of the Internal Revenue Service.

So collectively we have a great deal of experience and expertise on privacy. Let me begin by posing sort of a broad question about how each of you operationalize privacy in your organizations, if you could each give us a synopsis of what tools you find particularly important in your programs. If we could start with Jane.

MS. HORVATH: Sure. Thank you. Good morning. I'm pleased to be here.

I would say there are three different ways that we operationalize privacy within our organization. First and I would say the macro level is where my office sits within the organization. We sit in the Deputy Attorney General's Office, and there's a saying at DOJ that everybody reports to the DAG, which is essentially true if you look at the org chart.

So the DAG is aware of all programs and initiatives that are going on within the Department of Justice. So he's logically the one who can insert me into a program at the beginning or insert our office into a program at the beginning. That is essentially what we have arranged or agreed upon when I came on, is that really the only way to address privacy issues is at the start of a program.

It's very, very difficult to come in at the back end when something's either hit the newspaper or there's a crisis at hand and privacy hasn't been addressed. I would say that you have a very strong likelihood of losing the program or having it substantially cut if you don't look at these critical issues first.

The next thing that we've done with our office is we've established a privacy and civil liberties board, and on that board -- it's really specifically to address terrorism and national security issues that give rise to civil liberties and privacy issues. Sitting on the board are individuals within each component that have policymaking authority.

We have separated the board into three different committees: the data committee, the law enforcement committee, and the outreach committee. Those committees will meet once a month and the board will meet to basically endorse committee initiatives or if there's a crisis or a critical issue that it needs to address. The data committee right now is looking at the large issue of commercial reseller data that we have been recommended to look at strongly by a GAO report on commercial resellers. The law enforcement committee is basically a vehicle whereby law enforcement officials can bring different privacy or civil liberties issues to the board for us to address and then for me to take to the Deputy Attorney General or the Attorney General as necessary.

The outreach committee, which we also view as being important to operationalizing privacy, is actually reaching out to minority communities and letting them know that we understand their concerns and that we are not within our programs trying to violate their privacy any more than any average American.

Then I would say on the micro level we use the privacy impact assessment. We have basically lifted from the DHS guidance a new tool that they introduced, which is the privacy threshold analysis, which is a tool that we give to the CIO's office to look at any system on a small level and they can go through a checklist to determine whether the system that they're developing actually has privacy implications. Then after they fill that out would they then go and fill out privacy impact assessment.

MS. LEVIN: Thank you.

Zoe.

MS. STRICKLAND: Thank you.

You know, I often say that a Privacy Office, we're not just mini-compliance activities; we're not like a little mini-law department. In addition to compliance, which is obviously a very important aspect of privacy, we're also meant to be exercising and establishing sound policies and good judgment.

Examples are how do you do redress, how do you do risk mitigation and privacy mitigation? So we're meant to take on that role of exercising sound judgment, both in terms of what we see today as well as what's coming down the pike.

Of course, before you can operationalize privacy you've got to have a good understanding of your agency and who you are and what your requirements are. You've got to have those mapped in terms of what you really think the requirements and policy needs of your agency are.

When you have a good foundation for that, I would suggest at the very simplest level there are two ways to really operationalize privacy. One is getting your management or your agency to understand what you do and the importance of what you do. There are various ways to do that in terms of how you network. There's formal ways, like Jane was talking about, and we also have a privacy board of key functions who touch personal data from marketing to information security to Postal Inspection Service to IT. Get all those folks together and make sure that you're communicating with them, because I'll tell you, not only can they go out and tell their departments what's going on, but they actually improve your own policies and processes because they can tell you about the impact to them.

So you want to be able to build those formal and informal management networks.

The second way I call more tactical, which is how do you make sure that your agency is complying with your various privacy laws and policies that you put in place? It's very, very important. One of the fastest ways, as we all know, to get yourself in a lot of trouble -- true for private sector, too -- is to put a promise out there and then not having anything behind it to make sure it happens.

So make sure you've got a process in place for each one of these requirements. Typically, each agency has existing processes there. Information security has a process for new IT systems. Your purchasing or your supply management department has a process for contracts to make sure vendors are doing the right thing with personal data.

So go find them. A lot of times you can partner up with those guys. And then find where the gaps are and introduce a process there.

One of the questions for us here is they wanted us to give examples, so I wanted to give a couple examples from the postal perspective on operationalizing privacy. One has to do with Katrina and all the fallout from that hurricane. Obviously that was a massive impact on the country and particularly folks in Louisiana and Texas and the other localities. It became a real crisis.

How do we share data appropriately to help these folks? Because the Postal Service had a very strong framework for what was appropriate sharing and what was inappropriate sharing, we were able to do that data sharing within a week of the requests we got from other agencies. We had a certification process, a routine use process, and we followed that very closely, because I actually think good privacy is not just withholding data, it's also sharing it when it's appropriate to share it in the right way.

So we did the data sharing. We actually got visited by DHS, the OIG folks, to say, how did Postal do this? We also put on extra bells and whistles to it, too, because for instance -- a good hypothetical for folks -- we were approached by the state election board: How do we make sure that people who are not in the locality are able to vote? That was a key very important factor for them.

So again, using our routine use of the certification process, we did share with those officials. But we put in extra requirements that wasn't required by our routine use to say they could not share that data with anyone without checking with us first.

So that's part of how does your framework work and how do you add on things to make sure that you're meeting the goals of your privacy promises.

Another example, and I think this is a key one for operationalizing privacy, is -- I think we all love this one in the privacy community -- is when your organization comes to you with privacy questions and things they've read and seen. In a recent example, our marketing folks contacted us with the recent Direct Marketing Association's news releases around security breaches and differentiating different kinds of data, marketing data from health data and things like that, and the impact that has on your use of data, your marketing, your security needs. They were thinking about how do we segment data, and I thought that was just wonderful.

So I think it's just a very critical function for each agency to figure out, how do I operationalize and embed privacy within the organization.

MS. LEVIN: It's good to know that after all these years you're still working on new solutions and new policies.

MS. STRICKLAND: It's always something new.

MS. LEVIN: Harriet.

MS. PEARSON: Good morning. Thank you.

I think Zoe and I have probably been in our roles for the longest that I know. Six years or so we've been at this. So I am the private sector representative to talk a little bit about some practices we have at IBM and how you might think about using those examples in your area of responsibility.

So we're a large organization, so 160- plus countries, 320,000 employees, 100,000 contractors, lots of lines of businesses, integrating information, and more and more doing it in a globally integrated fashion, which creates challenges when it comes to providing access to data about individuals or even corporate entities or corporate information across borders. So we clearly have that issue in spades.

The way to operationalize anything is to start back with a strategy. So the strategy of the organization, the mission of the agency, what the frameworks created by the regulations are, etcetera. For us our strategy is very simple. It's got three major thrusts. The first one is all about ensuring that our policies and our processes continue to keep us a leadership organization in terms of how we manage data about individuals and organizations and how we keep it secure and private. That clearly is a huge plank of our strategy.

The second is, due to the nature of our business, is to be a leader in privacy-enabling technologies and solutions. We don't view it as a revenue opportunity, frankly. We view it as something like environmentally conscious design, something like that, where it is more or less an obligation I think of organizations, particularly I would submit government organizations, to think about these kinds of issues in designing processes and solutions.

For us, a new solution involving RFID might be the equivalent of something that you might be working on. So those are the kinds of things that go through our mind. An example of -- I'll give you examples in a second, but that's the second plank of our strategy.

The third one is really, because this issue, these issues, are evolving, there's always something new and the era in which we're living, whether it's because of the post-9-11 issues or the acceleration of what technology can provide or other factors, these issues are always changing. So it is clearly a part of our strategy to stay connected to the leaders, the organizations, the government agencies that are changing policies, that are making best practices and policies, so we clearly have an investment in that.

So when you operationalize those three prongs of the strategy, on the first one, which is about policies and processes, we have a global set of guidelines that apply to all employees. Privacy information, employee privacy, are a very, very significant component of it, reviewed annually, signed off by all employees, education provided to all employees via that mechanism, supplemented by a set of specific corporate-wide instructions or policies that apply to HR information and other kinds of major process information, supported by guidelines and really specific guidelines that apply to specific processes.

We don't have a PIA process per se, but what we do have almost looks the same, because it says if there is a new IT application or an application that uses data it does go through a quality checklist, a process, and embedded within it are those elements that start looking a lot like the DHS tool. But we haven't called it as such, but it's there.

It really goes down the essence of it, and we've actually started calling it internally - - we've started divorcing it from the issues of privacy, security, or whatever. We're just calling it data governance at this point. We're starting to call it what it is when you strip away and you actually get to, what do you do with data once it has a policy attached to it? The policy says you can share it with so-and-so or you can't share it or you have to apply this kind of security, or here is how long it can be retained.

Whatever it is, it just becomes a policy management exercise, and it makes it a lot simpler to actually implement when you actually think about it that way, because then the number of disciplines come together and everyone understands what you're talking about. So that's what we've started to do in our organization.

On the second prong of the strategy, around looking at technologies and solutions, some examples I'll give you. We have put in place a research organization that has scientists working on what kind of enabling technologies might be there. On RFID we've actually done some interesting work on, you can scratch the chip, the RFID tag, and disable it, and a couple of other areas like that.

In the area of health care and genetic information, we actually are doing some interesting work, and one of our policies we actually changed around that last year was in saying, you know, if an employer has access to genetic tests of an employee, however he came into contact with that information, what should you do? The U.S. Federal Government, I believe the agencies are covered by an executive order signed by the prior administration.

In the private sector it's not clear at all what the obligations are with respect to privacy and employment decisions. There are some state laws. There is no federal law. We said, you know, let's create a uniformity of approach here and actually let's make it global. So we actually committed to our employees proactively and changed our equal opportunity policies and our privacy policies that if we did come into contact with that information, however we did -- not that we're collecting it, but people share these things sometimes if you take a test that indicates a predisposition for a certain disease, a cancer or Huntington's or whatever, and you're looking for additional help with insurance or what-not -- we said, we will not use that to make employment decisions, we will not use it to deny health care insurance access, and that was driven out of the privacy office or the function.

So examples like that. Then finally, in terms of staying connected, there are lots of groups out there that have best practices that are full of folks who really are thinking through these issues on a day to day basis. It's pretty easy to avail yourselves of that network because it's still relatively small. I would say hundreds and hundreds of people, but all very willing to share, and I have found it a personally very rewarding process to be engaged in that thing.

But also, it helps keep you up to speed on where are the leading best practices. I think I would say the U.S. federal agencies are a leading best practice in terms of the PIA process. In terms of the private sector, I think we have a lot to learn from how you are doing it as well.

Thank you.

MS. LEVIN: I really want to say ditto on the concept of thinking of data governance when you think of privacy, because it is a great concept I think that captures a much bigger profile for how we want you to operate when you deal with data.

Maya, please.

MS. BERNSTEIN: Thank you. Can you hear me?

So I sit in the Office of the Secretary at HHS, in the Office of the Assistant Secretary for Planning and Evaluation. That's kind of the policy coordination arm of the Office of the Secretary. I'm not really an implementer of our policies, although that's sort of -- making sure that happens is part of my job. So I may have a little bit different perspective than my colleagues at the table.

I don't know if there's press in the room, but I am obligated to add that I am not speaking for the administration, the Secretary, or the Department. I'm here speaking from my own experience, but I'm very pleased to be here this morning.

At HHS we have very significant collections of personally identifiable information. We have 200 million people who are in our national database of new hires, which is related to the child support enforcement program, 42 million Medicare beneficiaries, 1.6 million American Indians and Alaska Natives who get services through the Indian Health Service. I'm not exactly sure how many people are covered by NIH's clinical and research centers or at CDC. We have our own 67,000 employees whose information we're responsible for.

All of these are covered by the Privacy Act. Some of them are also covered entities under HIPPA, under the HIPPA privacy rule. We also have our specialized rules that cover things like substance abuse and mental health records that have their special laws that cover them.

So there are certainly a variety of responsibilities that we have. On the day to day basis, I have to say that the officials that are carrying out these missions, it's their responsibility for collection, maintenance, use, disclosure of those records, and so privacy is really everybody's responsibility at the grassroots level of the agency.

There are kind of three prongs I think, and maybe I'm going to echo a little bit of what my colleague said. You need to have the right policies in place, you need to have the right practices in place, and you have to communicate with your colleagues, both inside the agency and externally.

So that having been said, the Office of the Secretary does exercise oversight review, policymaking functions, and they're kind of divided at HHS. We're not as centralized as some of the other agencies. The Office of the Assistant Secretary for Public Affairs is responsible for the Privacy Act and the Freedom of Information Act, so various kinds of public requests that come in. They're processing the requests for information, but they're also helping people to comply with the Privacy Act by drafting notices and making sure that those happen and so forth.

Our Assistant Secretary for Budget, Technology, and Finance is where our CIO sits. That's our senior official for privacy, our CIO. The CIO has determined that it's appropriate to designate senior officials, not only at the Department level but at each of our operating divisions, so that we kind of have a network that filters down, that there's a communication process back and forth.

That office also has responsibility for our privacy impact assessments, and I have to say that that's been a change certainly in the last five, ten years since the IRS created the concept. That is a real key for us. HHS policy requires a privacy impact assessment on every system, every system regardless of whether it contains personally identifiable information. Part of the reason for that is that you can't really know if it has personally identifiable information unless you do the impact assessment.

So in the case where there isn't personally identifiable information, there's a little summary, we post it on the web. You can see that we've looked at it. It's much longer and more involved in the case where there is personally identifiable information. I think that that allows us to get in -- earlier I think maybe it was Zoe, you were saying that the point is to get in early and up front. You don't want to have to be retrofitting or backtracking. It's going to cost you money and delay in developing systems or putting policies into place. You have to ensure up front that your practices are in line with your other policies.

Then in the case of my role, Toby sort of mentioned it a little bit. Basically I'm doing forward-looking policy development. We're monitoring new technologies and programs that may give rise to privacy issues, identifying areas where there's a need for privacy policy, advising our policy officials on things that stem from administrative initiatives.

Even though I personally don't have staff, I have other mechanisms through which I can get the job done. In ASPE we have a kind of central review function, so legislation, regulations, other kinds of policy documents of the Department are coming through that office. So I have an opportunity to kind of grab at them, identify where there are privacy issues, and work together with my colleagues in the operating divisions to figure out what the right policy should be or whether they have -- I can sort of flag issues that come up and say: Well, have you thought about this? Then I can dig a little bit deeper and say: Well, you're asking me to create a Privacy Act system of records for something, but can I see the documents that you're using to collect the information, can I see? And it turns out you find things that way.

The second is that we have a data council at HHS. So there are representatives of all the operating divisions. We coordinate research programs. We coordinate essentially the use of data at the agency, which I mentioned there's lots of it. Under it there's a privacy committee. There are representatives of privacy from each of the operating divisions. This is sort of part of the communications part.

These committees, and there are a variety of them of various sorts -- there are also some on particular issues. So for example, HSPD- 12. You all know we're going to get new badges. So there's a privacy committee just focused on implementing HSPD-12 and making sure that in the design architecture, starting from concept all the way through implementation, that privacy is worked into that process.

There's a federal health architecture privacy and security group and that one's actually inter-agency. I chair it with a colleague at the VA who's been a little busy lately. I haven't talked to her in a little bit.

We also have a small bit of money to contract out things where we have special projects. So we have various mechanisms. But basically those three arms. Part of it is making sure you have the policies in place, part of it is making sure through the PIA process and some other processes that you have that the practices that you have are matching up with the policy, and the way to get that to happen is with communication.

So I have this convening role and part of it is I can disseminate information to my colleagues and part of it is they can tell me what's happening out there. They can be my eyes and ears out there among our agencies.

I guess those are sort of the three prongs in the way that we implement it. It's sort of high-level.

MS. LEVIN: I think that is very helpful.

Let's turn now to privacy impact assessments. The mere virtue or the fact that we're holding this workshop today indicates that the DHS Privacy Office thinks that privacy impact assessments are critical. They are very much a core tool that we feel the Department can use to operationalize privacy.

But I wanted to hear from our panel today how you use PIAs, if you do, and are there times where PIA's are most helpful, or are there times where they are not as useful a tool? Zoe, start us off if you would.

MS. PEARSON: I love this question. Are PIAs useful? Well, absolutely. This is something that I think a lot of us were doing, to Harriet's point, were doing already before the government act occurred, because if we're going to be collecting data in various systems and we have these existing legal and policy requirements, we want to know what's happened to that data and make sure that you're complying with your laws and policies. So it is absolutely a useful tool, particularly for things that the public really cares about, which is these largescale data collection systems and how is the data being collected, what's the data in there, how's it being secured obviously is a growing issue, how it's shared. All those things are very central.

For Postal Service, we partnered up with the information security folks. They already had a process for new IT systems for all the security pieces, called their information security assurance process. So we partnered with them and we created some sections devoted to privacy, and then we also have a few that are a little bit of overlap of privacy and security.

For Postal Service -- and by the way, you're welcome to take a look at our tool. It's on our website, usps.com. It does all our privacy needs there. We did a combination of Q and A's and open-ended questions so we could really get a good understanding of what was going on and sort of drive behavior. Examples of specific questions were: How long do you keep data? Tell us? Things that are more open-ended is: How do you dispose of that data at the end? Do you have contractors? What are their names? So we can then make sure -- and have you included the right privacy clause? And if not, we can go back and make sure that that's really happened.

Then also driving behavior, like: If you collect more information, particularly more sensitive information, well, that increases dramatically your security requirements and your costs and your time frame for implementation. Oftentimes driving behavior helps when you're talking their language a little bit, instead of saying: Well, here's a requirement and I said so. It helps to sort of explain what you're looking for and the behavior you're trying to get to.

One thing I really like about the PIA process for the federal sector, and this is real kudos to OMB, is the flexibility they allowed for agencies to develop the appropriate tool for the agencies. If you look around at each of our agencies, there are certain things that are more of a critical risk than others, and how do you make sure your PIA handles those things very carefully.

I know when Maya was at IRS one of the big issues they had was minimization: How do we make sure we minimize data? For Postal a big thing is how do we use data to do marketing or sharing? Homeland Security obviously has a set of issues that they're faced with and a lot of public scrutiny.

So take a look at all the tools out there and see what makes sense for your agency and tailor it. Postal Service, ours is scalable, so the more complex, sensitive systems, we get more information, more mitigation. We have a simplified tool for the field because their IT systems, we learned from them, are much simpler. You can do much more of a template for them.

The second part of the question is when is a PIA not useful. It would be great to say that you could use a PIA for everything, and you can make it a major tool for the majority of your needs and it would be useful in almost every aspect. But some examples of where you need to think about additional elements are things like data-sharing, that don't involve, you know, someone asking for a computer match or something like that. How does that happen?

Or how do you do notice? In the Postal Service we collect personal information from every -- we call them channels: from the phone, from email, from forms, from the web. How do we privacy notices in each of those channels?

What we do, for our PIA tool we break out the privacy sections and use those against things that aren't even IT systems. But you do need to take a look at other processes that are in place that you can partner with. I mentioned contracts is a good example.

I think one thing we're all going to be thinking about in terms of looking forward, the issues that are coming down the pike. There's a bill on the Hill right now that requires a privacy impact assessment for every proposed or final rulemaking. Have you all read about that? Yes, and that's a separate privacy impact assessment that needs to be done for both proposed and final rulemaking that involves the collection of data on ten or more individuals that are non-employees, and individuals under the bill are allowed to go in and seek judicial review if they're not satisfied with the PIA you've put in there, which I think will be very interesting to see if that played out.

So far, we haven't seen yet how all these pieces -- OMB is here to give us all this excellent guidance on how all these pieces fit together, because you've got your PIAs for your IT systems, you've got your computer match, you've got your Privacy Act, and then you've got your PIA for new rules. How does that make sense, and at what point are you, in your reports and plans, are you really communicating effectively with your constituents and the public, how do they fit together is something we really need to think about.

MS. LEVIN: Well, the Homeland Security Act provided DHS with, the privacy officer, with that authority to do PIAs for proposed regs. We have some experience with that. When the rest of the Federal Government catches up, we'll be happy to share that.

This afternoon we'll be focusing a great deal on mitigation. So I think identifying risks and figuring out how to do mitigation is something that we hope you will turn to our office for assistance with in doing your PIAs.

Anyone else want to add anything on PIAs before we move on?

(No response.)

Yesterday there was a hearing before the House Committee on Veterans Affairs on a subject I am sure you are well aware, and the GAO in its testimony said: "In addition to establishing a robust information security program, agencies can take a number of actions to help protect personally identifiable information from compromise. A key step is to develop a privacy impact assessment."

So from there, let me ask: To what extent has operationalizing privacy and operationalizing security, a distinction between the two become meaningless? Can you operationalize one without the other? We'll start with Harriet so we can see it from the privacy sector perspective, how that would work.

MS. PEARSON: I'll harken back to my comment earlier that at some level this becomes -- taking data and making sure that it's managed in accordance with the policies that it needs to be managed to becomes an exercise that you need to -- we're almost calling it something different. You can pick whatever name you want. It can be policy management, it could be -- we're starting to call it data governance.

But it is managing the data. That is one way to look at it. I think you cannot ensure that the privacy expectations of your constituents are met unless the security of the underlying process -- unless security is also achieved. So simplistically, I have always used this little pyramid and I've shown the privacy thing at the very, very tip of the top and this massive pyramid underneath, which is the security of the information processes and the other kinds of processes.

You cannot achieve the privacy without security. So in a sense, harkening back to the opening speaker, the Assistant Secretary, you've got to put them both together. You just have to. So that's -- I think it's pretty clear that you have to.

We have taken actions around minimizing the risk of information being misused. Even very simple things go a long, long way. A lot of this is really dealt with by education, by communications internally, raising sensitivities, having people think about these issues and making sure that when they go home and talk about things at dinner that they are able to say: Hmm, this is what I'm doing; we've thought about all angles.

We even did something simple several years ago. I like using this anecdote because it's very simple. The number one issue I was getting notes about from our own employees was: I keep seeing the SSN, the social security number, being used all sorts of places. You guys ask for it everywhere. Anything I need to do, whether it's to download a web form for adoption assistance, where, by the way, it wasn't the actual process to get the adoptions, it was just getting me the form, or calling an 800 number to get something, people are asking me for my SSN to authenticate, and that doesn't make sense.

I said: Yes, they're right, it doesn't make sense. This was four years ago now. We did an inventory of what are the processes that are asking for SSNs. We found it was like hundreds, and we started paring back, paring back to what we thought was the absolute core number of those processes in the U.S. that we needed the SSN to do whatever, whether it was to administer health insurance claims or whatever it was. We pared it back.

Then we did something where, you know the cards that you carry, the health insurance cards. You used to have, a lot of the private sector health plans used to have the SSNs right on it. They used to print it on envelopes, they used to do all sorts of things. We went to our, at that point I think it was 150 health plans that we contract with to provide health insurance benefits, and we said: By X date, by July of 2003 or something, please stop using the SSN on visible pieces of identification and things that are not secure; it's not acceptable any more.

They said: We have never heard this before. We said: Well, this is our new policy. It was interesting, this back and forth. There were a small group that did not want to do it and to them we actually wrote letters and said: This is something we are going to start using in determining whether or not we purchase. And then pretty much all of them followed suit.

So it was an interesting little -- and it was very simple to do. It was partnering with the human resources group, educating them about why these are issues, and very, very effective with the workforce. The workforce noticed, it noticed. Even to this day I get lots of emails about: We're glad we don't see this, or why is this person asking for my SSN? Then we have to explain that it isn't an identifier that is used, and we just need to understand that when it is used it needs to be used in a secure fashion.

So that's an illustration.

MS. LEVIN: Maya, other examples?

MS. BERNSTEIN: Yes, I think there is still a distinction between operationalizing privacy and security. Security we traditionally think -- the security folks that I work with traditionally think of their responsibilities in the areas of confidentiality, integrity, and availability of the information that's in their charge. As Harriet said, that's a foundation. You can't have the protection of privacy without making sure that those things are protected.

But privacy has other things as well. What you collect in the first place, the security people don't usually think about that. That's a program issue, what am I going to collect, is what I'm collecting relevant and necessary to my mission, is it, at the IRS, is it the minimum necessary information that I need to collect?

On the one hand, that's a program issue. It's not entirely related to security. On the other hand, if you don't collect it, you don't have to protect it. So it's related to security in that sense.

Making sure that you don't have secret recordkeeping systems, that is for the Federal Government publishing a notice in the Federal Register. Not really considered a security thing, but in terms of your operation you better do that or you're violating the law. Giving people individual notice on the form as part of your collection mechanism, that's a privacy thing, not usually considered a security thing, although it does help people understand if you describe in there what the security controls are for your information.

Your right to access and amendment is an important privacy right, but the security people -- I guess they need to think about it so that your information is available when you ask for it. But they're not the people who are implementing your right to access and amendment.

Whether your information is accurate, relevant, timely, and complete, that's a sort of double-edged thing as well. So there's a relationship between them, but I don't think that they're entirely the same.

I had one of my colleagues, a high- ranking, very smart colleague who was involved in architecture at the IRS. I gave a talk to a group of architecture folks and he sort of had this wide-eyed view at the end of my talk and he said: You know, it would never occur to me that privacy people think about what you collect. And I thought this was amazing. It was so obvious to me as a privacy person that what you collect is so important, and to him at the IRS, we have to protect what we've got, but what we collect is somebody else's problem.

So I think, jumping off of also what Harriet said, I think there is a cultural change or a certain infusion of the culture that Harriet was describing that we have to work on, making everybody understand that it's part of their business, making them be able to easily talk about it when they go home and talk with their families about what they do over dinner, so that it's easily understandable and it's really infused into every piece of what we do.

I think that that cultural change in some agencies has worked better than others, and for those of us -- for others, that it really has to expand. Part of that is communication, part of that is just -- I guess a lot of it is communications, getting the word out, making sure that people understand in their day to day work and making people understand that it's also their data. We're talking about employee data as well, and it affects them, not only the programs that we're running.

MS. LEVIN: Harriet -- go ahead.

MS. BERNSTEIN: It's more of a general philosophical point. The cultural point here I think is so important, and I don't know how many of you have kids or friends who are out there blogging or chatting out there or myspacing, or whatever it is. We've got an interesting evolution here that we're going to go through as a society as we grapple with the realities of a post-9-11 world, and they are there, but also as we, especially as the younger generations, who are very comfortable in social networking and sharing information about themselves -- we've got to somehow bridge and create a culture within our government, within the organizations that have responsibilities, and then ultimately the people who work within those organizations to know that data matters, that handling data responsibly matters.

I've used this analogy multiple times. It's akin to having your kid come home from school and talk to you about recycling and how important recycling is because they're learning it in school and they're learning it in places. We are going to see that. I think we kind of have to get there.

These data breach incidents that have been happening so frequently recently are really going to drive us there, I believe. People are going to say, well, have you shredded, have you done this? That will prompt those kinds of conversations and open up the ability for professionals who are in the business of securing this and acting, ensuring that the systems are in place to go ahead and do what we need to do.

MS. LEVIN: Zoe, go ahead.

MS. STRICKLAND: I think all of us feel so strongly about this issue, about the cultural change. To Maya's point about changing the culture within the agencies, that really is key, because I tell you, the culture has changed externally. The media cares a lot about this, employees care a lot about this. We get the same emails on the SSNs. And customers and the public care a lot about this, too.

We get questions like: Why is my account number on my receipt? Never used to get those questions. There's a new way that the public is looking at this and thinking about this. So if we're doing privacy the same way we were 20 years ago, we are not really meeting the needs of the public today and listening to what Congress and the media and all those other sort of intermediaries are trying to tell us. So we need to think about that.

MS. LEVIN: Jane.

MS. HORVATH: I have one thing to add. Right now the Attorney General has directed that the Department look at the idea of ISP data retention. I'm not going to go into the merits of that, but I am going to tell you how we've handled looking at it and how that kind of reflects a cultural change of looking out, as opposed to just working within the Department on this issue.

We've had various representatives to ISP's come in and give us their opinions on what they think about ISP data retention. And more important to my role, today at 1:30 and two weeks ago we had leading representatives of many of the privacy advocacy groups come in and we shared with them what we were thinking with regard to ISP data retention, which has tremendous privacy issues, and allowed them in open forum to talk to senior leadership within the Department about their concerns.

I think it's a very good way to educate -- bureaucracy has a tendency to be inward-looking and not look out and be aware of what's going on. So I view my job as also bringing the outside inside and making them aware of issues that are timely, in the news, or of concern.

MS. LEVIN: I'd like to think that perhaps the concept is that data governance, which definitely can be focused on privacy, including security, not to minimize the important role of the information security part, but it's almost like we have to keep looking a little bit broader, a little bit broader. To do adequate security you've got to also consider privacy, you also have to consider data governance.

Many -- I won't say many. Maybe a few program managers in our audience today, hopefully just a very few, think of privacy as simply a hurdle that they have to go through in order to get programs approved and perhaps don't really see, in business terms, a return on investment. I'd like to ask our panel: From your perspective, is there a return on investment benefit to programs that do privacy well?

Jane -- Zoe, I'm sorry.

MS. HORVATH: It doesn't matter.

MS. LEVIN: It doesn't matter, okay.

MS. HORVATH: I will take a quick shot at that and I would say absolutely. I would say as I came in in February there were quite a few articles in the newspaper, and while I was interviewing for the job I'd pick up the newspaper and say: Yet another issue that the Department was grappling with, Patriot Act re-upping, etcetera.

I find that my office is called very often into meetings and into programs because they've realized the value that looking at privacy, civil liberties protection at the outset will provide to them in getting a program approved. So I would say there is definitely a return on investment.

MS. LEVIN: Zoe.

MS. STRICKLAND: I think for some folks that privacy is a checklist item. For some folks that'll be true, who you work with. And if that's the case, well, so be it and you'll work with those folks to make sure that things are done correctly.

Obviously, we're all working on the hearts and minds of the folks we work with and you do want to get the understanding of your program and to make sure that they understand the value and how it's actually helping meet their needs as well.

But sometimes you will run across folks who have a checklist mentality and there -- I loved Harriet's example of how you drive the behavior, because one thing that's not helpful is when you say, well, here's our requirement, and they say: Well, here's our requirement. And then you've got little requirement warfare, whose requirement wins.

The more you can talk to them about how this meets, A, the legal needs, but also the program needs and the public needs and talk their language, it really does help make it effective.

In terms of metrics, I think you can look on the negative side and the positive side. I think most agencies, including Postal Service, we're comfortable in the sort of cost-cutting and cost-saving role side of metrics. Examples of things that we use, because we've gone to this performance-based evaluation system where you have to show metrics for our programs, is saved work hours when we redid all our Privacy Act systems. We didn't have to slow programs down and spend hours doing these Federal Register notices.

You really can save quite a lot of costs. VA is now, as we know, looking at all the ramifications of what's going on and speculating about the fees and costs they're going to incur. But my understanding from some press reports is that they've already spent $25 million on the call center alone, with the hundreds of thousands of phone calls that they've gotten.

MS. HORVATH: The number I heard was 260 million --

MS. STRICKLAND: Some of that is --

MS. HORVATH: -- just in plain envelopes, you know. Really, they had to go out and procure 26 million envelopes. What's the cost of that? When you're talking about a privacy breach you don't think about these things, but it's very expensive.

MS. STRICKLAND: Right, and what sort of claims and injuries are they going to hear from folks?

So you have either costs you're trying to avoid or, as was mentioned earlier this morning, having your program slowed down or halted if privacy isn't done well. I think an example of how people have changed how they do privacy, I think Homeland Security gets a lot of kudos for that, because if you compare the Federal Register notices they write today and the announcements they do today to some years ago, it's a noticeable difference.

On the plus side of metrics, there's some movement there, too, to say what is the ROI for privacy? Postal Service, because we have, we sell products and services, we've done a lot of customer surveys around our privacy in terms of what do you think of our website privacy, our email notices, etcetera, etcetera. We've gotten a lot of feedback from that in terms of making it better.

I know other groups are also looking at how do we measure ROI. The Parliament Institute is taking a look at is there a connection between trust in an organization and how responsive are they to either marketing messages or to doing business with you as a company or an agency. I suspect we'll see more of those kind of studies being done.

So for us as privacy officials, we want to try and push both ends: the cost avoidance, the problem avoidance, plus the increase in trust and the value that has to our constituencies.

MS. LEVIN: Maya.

MS. BERNSTEIN: Yes, I was just going to say, jumping off from what Zoe said, that measuring trust is a very difficult thing. In previous agencies I've been in, it's hard to sort of justify your existence. Well, what is this getting us in terms of dollar value. Measuring that comfortable good feeling that people have when their privacy is protected, that's a very difficult thing to measure.

Yet you kind of know when your programs are working smoothly, when there's not -- it's sort of easier to measure the negative impact than it is to measure the positive impact, and that's a challenge for people, I think, in the privacy area in terms of justifying their budgets and just understanding the bottom line for management.

MS. LEVIN: The recent incident of a VA employee's laptop being stolen I think highlights that the human link can be the weakest link in a security program. So that assuming you have the privacy and security policies in place, what more has to be done in order to help prevent those types of incidents?

Jane, do you want to chime in here?

MS. HORVATH: I would say the best security and privacy policies are only as good as having your own employees knowledgeable about them. So if you don't train them, make them aware of them, and really take it down to their level -- we were having a conversation recently, a lot of the private information that the DOJ handles are case files. There really wasn't a realization in the U.S. attorney community that, oh, you know, when I take a manila folder out to a courthouse that's actually Privacy Act-protected material.

It's really taking it down to a micro level to make them an owner in this process, and also make them aware of the damages that the agency could suffer monetarily if there is a Privacy Act violation. So I would say using -- we have a broadcast email facility that we use to send messages out to employees and we're going to be sending out a notice next week that I'd like to do by broadcast email, reminding employees of how to treat secure private information and departmental assets in response to the VA data breach.

MS. LEVIN: Hopefully, all of our DHS colleagues recall the announcement that was sent out by our office in conjunction with the CIO's office at the end of last week, because we felt that it was a very important time to repeat that information. People may not have had it in their front and center.

Anyone else on terms of how you might go about doing that? Maya?

MS. BERNSTEIN: The point you just made I think is very important, that is repetition. You've got turnover in your agency. You do have some very long-time colleagues, but you can't make a cultural change at once. You have to have reminders, regular communication reviews, updates on a regular basis, because there is turnover in certain areas and the report are new things that crop up and things that change over time.

So you can't just set your policies in place and think you're done. You have to keep doing it. It has to be a constant part of the program. It has to be worked into kind of the everyday.

MS. LEVIN: Harriet.

MS. PEARSON: I'll add one more thing, which is clearly education and communication is critical, but at some level I know our colleagues have discovered this inside our company and I'm sure it's true in all organizations: All of us are fundamentally lazy and I think, even if it comes to antivirus protection and have you installed the latest thing or whatever it is, people somehow just don't get around to it, you know.

That's where what we've done is automated stuff, automated tools that push things, that install things, without the individual having to take on the burden. So my point is, and it's sort of a supplementary layer to education, culture change, etcetera, there probably needs to be some new paradigm or new thinking or new tools or new whatever to automate the processes as much as human possible in order to keep striking the right balance between efficiency and doing what needs to be done.

It harkens back to, the better we actually -- it's a productivity issue, it is an economic competitiveness issue, frankly. At a country level, I think it is important for us to keep going for those kinds of improvements so that we don't impose more of a burden on our processes, on our productivity, as we might otherwise do.

I think, especially when it comes to security initiatives that are going to be data- intensive and require the collection or the scanning of lots and lots of data, that's also an opportunity, I think, for new paradigm thinking about, well, do I really need to see what's underneath, do I really need to see the individually identifiable pieces of data, or are there other ways to get to the same result?

That may not be the province of a Privacy Office per se, but the locus or the center of competence that the privacy function develops certainly can be useful in advising, assessing, and helping the colleagues in whatever organization that you're in do that kind of thinking, help provoke that kind of thinking.

MS. LEVIN: Well, our office often talks about anonymization as one way in which you can mitigate risks. So that definitely would be a tool.

Zoe.

MS. STRICKLAND: I do think, on this area -- and I think that's an excellent technology tool -- is an issue that both the private sector and the public sector is facing - are we going to require notices when there is a security breach? This is a major conversation now on the Hill and within both the private sector and public sector: Are we going to adopt this as a matter of policy even if it's not driven by a legal requirement?

I think that debate is going to continue very heavily. It's interesting to see what the features are, what that notice would look like. Frankly, we all know that there have been security breaches. It's not like all of a sudden these things just started happening last year.

Where does that put agencies? There was a recent report, I think with NSA, where they had a security breach a year ago and they didn't do a notice, and now it's coming out in the press saying: Geez, they've known about this for nine months or a year; how come this wasn't reported? I'm sorry, DOE, DOE. My apologies. My apologies to NSA. It was certainly one of the agencies recently.

MS. HORVATH: You don't want to give them any more.

MS. STRICKLAND: But the thing is I'm sure they're saying, and I would imagine Postal might have been saying hypothetically, is there wasn't a requirement to do a notice at that time and do you want to create one? We're certainly moving in that direction.

One thing that agencies have to face the private sector does not is that we also have the FOIA. So when we're collecting information about these security breaches, the extent of them and whether or not we're going to do notices and things like that, we can get FOIA requests from the media and from the public saying: I want everything you've got on any security breach you've had and your plans around it. Obviously you can withhold some of that, but that's something we have to think about as well.

MS. LEVIN: Let's then now turn to I think sort of a final question: What do you think are the difficult challenges to privacy implementation? Is it leadership, management, budget, education, training? A quick response from each of you and then we'll see if there are some questions.

Jane.

MS. HORVATH: I would say that's a loaded question, but all of the above, I think. A lot of it is just figuring out how to do 365 days of work within a week, because there is a tremendous amount out there that needs to be done. So I would say time, resources, and also making sure that you have buy-in from leadership and you don't get isolated, that you don't undermine what leadership is trying to do and that you're always looked on as an asset, as opposed to a naysayer, because getting isolated would probably be the biggest risk to a

Privacy Office and then that would create an atmosphere within the agency where maybe they do look at privacy and say, oh, this is just a checkmark I need to do.

So you need to always reinforce that you're an asset to the agency.

MS. LEVIN: Zoe.

MS. STRICKLAND: I'd like to obviously agree with that. I think you're going to get the same answer, the SAT answer, all of the above on those. I do think that a very critical piece, to Jane's point, is time management, because we do have more work than you can reasonably do an A- plus job on all of it. So we've got to prioritize our needs and our risks.

Take a look, and again to Jane's point, about what is the organization trying to do? Is this a high need of the organization and low risk? Weigh those features against them and figure out what you need to do. An example in Postal Service, when we put out a notice on the first national level commercial database that we acquired to support mail operations, very important to the organization in terms of mail processing, to make sure we're delivering to right addresses, but also obviously it gets a lot of scrutiny in the public, the commercial databases.

So we devoted a lot of resources to that and did do an A-plus effort on it. A lot of time getting the Federal Register together, brought privacy advocates in, and were able to proceed with that program.

Other things might be very important to the organization, lower risk. So how does that work? How do you make sure you're not slowing down and halting what the organization is trying to do, because they don't operate in a risk-free world, the program managers, the security folks, and privacy doesn't either. So we've got to try and figure out how we can make sure we get the needs of the organization met and making sure that we're meeting the privacy requirements to make that happen.

MS. LEVIN: Harriet.

MS. PEARSON: Agreed. One simple tool that might be useful is, all consultants use two by two matrices and there's always a magic quadrant. I think plotting those out and actually graphing for yourselves and your team what falls in that high importance, high urgency, must do area, most benefit to my organization, probably is not a bad exercise to do.

Just from my perspective, to add to that, there are two critical features and if you don't have them they're impediments. One is senior leadership support, which this is not going to work as well or at all if you don't have that. I think if you've got legislation behind you and a compliance requirement, you're going to have to do the mission, but it's so much easier with some senior leadership support, the roadways that get cleared when you have that.

The second is skills. Budgets, organizations, are almost secondary. If you've got people with the right skills and senior leadership support, you can move mountains in any area, and I think in this area too. Skills, especially as you try to implement and operationalize this in broadly dispersed organizations, I dare say we're running out of people who have deep, deep appreciations and we've got to do training like this and others to bring more people into the discipline, because it's cross-disciplinary areas.

So finding people with the right foundation, getting them skilled, certifying sometimes. There's a certification program out there for government folks. But in general just getting skills together and in your camp is really key.

MS. LEVIN: Maya.

MS. BERNSTEIN: I was on a panel last year with the industry advisory committee and one of my colleagues on the panel, I think he was the Deputy Director or Deputy CIO at DOE, used a phrase that really resonated with me that I remember. He said his focus was moving to the left of boom. What he meant by that was focusing on the proactive rather than the reactive.

We have a tendency to want to regulate after something bad happens or want to fix the problem after something bad happens. I think what we really need to do is change the focus. It's good to think about breach notification, but

I'd really rather not be thinking about breach notification. I'd rather be thinking about avoiding breaches.

So I think part of the shift that we have to continually do is to move to a proactive state, identifying problems up front so that we don't have to get to the right of boom. I don't want to say we never need to do breach notification. Realistically, it's going to happen. But moving my agency and moving my colleagues to thinking about how they can prevent that, if you want to talk about it as cultural change or communication or getting the leadership, all of those things are driving toward that change, toward that shift.

MS. LEVIN: Do we have any questions?

MS. HORVATH: Right behind the pole.

VOICE: (inaudible).

MS. LEVIN: We had asked that you put them in writing, if you don't mind. That's fine. You have the card in your packet, if you wouldn't mind.

First question: Does U.S. Postal Service post their PIAs on their website?

MS. STRICKLAND: That is an excellent question. We have a list of -- we have our PIA template posted, so you can take a look at that, and we have a list of all the PIAs we have done. We don't actually post the text of those, but they're available upon request.

MS. LEVIN: This is a very technical question: How should privacy be addressed during entire system life cycle, besides operational phase? For example, test data during proof of concept, pilot, development, contractor test facility, disposal, tape backups, archives and record retention, warehouse, etcetera? Typical system owner may not have full control during other SLM phases.

Wow. Who wants to tackle that one? Maya.

MS. BERNSTEIN: I think at the IRS, the model at the IRS actually works really well. They have for large procurements, say like tax system modernization, they required a PIA at every aspect of the process, I mean start at every milestone. The contractor who was putting together that system could not get to the next milestone without doing a PIA, among other things.

There were, in a sense, things you had to check off, but you had to go through an independent office, the Privacy Advocate's office, to do that. That started at the conceptual phase and at every milestone from design, when they pilot tested, all the way through the life cycle of a large procurement.

I actually thought that was a pretty good model. It allowed to review and revisit whether privacy was being addressed at every major step in the process.

MS. LEVIN: I think, as you'll find from this afternoon's tutorial, we also think that the PIA is not something you do in the beginning and then put it on the shelf. That's really a risk that you'll definitely get into trouble later on. So it's something that probably has to be done throughout the program itself.

How do we eliminate overlapping and redundant efforts between PIA and information security assessments? Both are labor-intensive and impact program budgets. They have the same objective. Both deploy basically the same technical controls, procedures, policies, etcetera.

Jane.

MS. HORVATH: I can take that. Like Zoe said at the Postal Service, we have worked with our FISMA security director to automate our PTA process into the FISMA questionnaire that every person who's developing a system has to go -- is supposed to go through before they begin the actual coding of the system.

So they'll go through the FISMA questionnaire online and there'll be a box that will take them to the privacy threshold analysis, and if they go through the threshold analysis in it and it indicates that they need to do a privacy impact assessment then that form will also come up. So we've actually combined it into the FISMA process.

MS. STRICKLAND: If I might add, that is an excellent question because one of the fastest ways to aggravate your organization is to say, okay, here's one set of processes, go answer these, and by the way our own office has a separate set of processes, go answer these. And they're like, well, some of these are the same questions; why is this happening and how does this impact my time frame, etcetera.

I think it's very -- a sensible thing to do is to sit down with them and map it out, because there is not a 100 percent one for one overlap. There are some things that the privacy office is going to care about, the security folks are not going to care so much about, things like how do you do your privacy notice, how do you give access to data. Again, there's a different perspective there. How do you do redress, how do you do mitigation?

So there are issues that privacy will want to take care of and address through the life cycle of the document, and there are things security is going to care about, and you want to rely on their expertise around firewalls and data security and things like that. There is some area in the middle where both folks are going to care, like who has access to the data internally and how is that data shared. There you just map it together and say, let's ask it once and ask it well.

One thing you can do for your program managers too is again mix the specific questions with the more open ones, open-ended ones, because if you ask them, what do you think about privacy, you don't know what you're going to get back. You want to help guide them around what are the issues you're looking for.

The DHS guidance gave some great direction on how do you get a specific sort of approach and answer to what you're looking for. But do sit down with them and map it out. Both your functions will be happier because you'll get better answers and faster answers, because it'll be built into how the IT system is developed, and the program office will be happier, too.

MS. LEVIN: Let me sort of combine two: In light of the VA breach, why not encrypt all privacy data; and do you feel more stringent privacy protections are on the horizon due to the breach?

MS. STRICKLAND: I'll do a quick answer on that one. This goes to the issue about risk avoidance and mitigation, how do you show ROI. Encrypting all data is enormously expensive. Is this something your organization wants to step up and do? Or do you want to take a look at encrypting certain types of data or transmissions of data? How does that work?

Another conversation you want to have with information security and the program folks, because it does cost some money to do these kind of things.

MS. LEVIN: Harriet.

MS. PEARSON: The other issue is I think there are ways to protect data and getting too specific, like the legislation pending has the word "encryption," some of the bills have the word "encryption" in them -- it's not necessarily only one way to ensure that the data are secure.

So it's not a binary, all or none; or maybe even putting something under lock and key and ensuring that only the right people have access to it may be just as effective.

MS. HORVATH: The other problem with encryption, as many of you programmers know, is when you encrypt the data you also have to de- encrypt it to use it and that takes time, and the more data you have the more time it's going to take to de-encrypt.

MS. LEVIN: When dealing with interconnected systems should a PIA reflect uses of data strictly for the system, the PIA it's being written for, or all interconnected systems? Systemcentric versus transparent processes.

MS. STRICKLAND: That's also -- all you guys are asking the right questions and I imagine the workshop will have fun going through some of these in more detail. Again, that happens a lot, like in Postal Service we've got a customer data warehouse. A lot of systems feed into it, because one of the things organizations are moving away from are stovepiped systems.

You need to be doing a better job of understanding and using the data that you have. Oftentimes government, we hear both things, which is understand and use your data better, and by the way, we're a little worried about data-sharing and how that's done.

So you want to take a look at -- I personally think you want to take a look at what is your business need and write, not just your PIAs, but your Privacy Act systems, around that too, because system names change. They modify, they evolve systems, develop. What you're trying to do is a certain activity for your agency or for the public.

So you're going to have some fun figuring out - how do I scope this particular PIA out, where do I draw the line around this particular box? But that's part of the planning process. And do think about it as a business process.

MS. LEVIN: I've been given the hook. The rest of the questions are fantastic, but they would really warrant much longer answers.

To have a culture of privacy, we do need leadership. In my unofficial capacity I'm now designating all of you, as a result of this panel and the rest of the day, as official privacy leadership proponents of better data guidance, data governance, and privacy, including security. So hopefully you've benefited from this panel and let's give them all a big hand.

(Applause.)

MS. LEVIN: We'll now have a 15-minute break. There is coffee or water and some other drinks across the corridor and feel free to use those, and the restrooms around the area. Thank you.