The Privacy Office
Department of Homeland Security
Privacy and Technology Workshop:
Exploring Government Use of Commercial Data for Homeland Security
September 8-9, 2005

OFFICIAL WORKSHOP TRANSCRIPT

Thursday, September 8, 2005
Auditorium
GSA Regional Headquarters Building
7th and D Streets, SW,
Washington, D.C., 20024

PANEL TWO
WHAT ARE THE PRIVACY AND LEGAL ISSUES RAISED BY GOVERNMENT USE OF COMMERCIAL DATA?

Moderator:
Ms. Elizabeth Withnell

Panelists:
Mr. Bob Gellman
Mr. Ron Plesco
Mr. Frank Reeder
Mr. Ari Schwartz
Prof. Daniel Solove
Mr. Tim Sparapani
Mr. Michael Vatis

MS. WITHNELL: So we can start with the second panel. We have some extra seats in the front in the reserved sections. So feel free to move up a little bit, or if you're standing, you can take some of the extra seats up front. Can you all hear me? If you will all come in and take your seats please. There are some seats down here if you folks want to move in. I spent the time during the first panel sitting in the back of the room so I can tell you from experience that on my left the microphones don't work as well, so I'd ask the folks on the left to please speak up into the microphones and if people can't hear to let us know and we'll be happy to see what we can do to adjust. I also think for the people in the back of the room that it would be helpful to introduce ourselves. We're the second panel. Our names are listed in your program. Our biographies are there as well. I'm Liz Withnell, Counsel to the Privacy Office. I want to welcome you to our second panel to

discuss the privacy and legal implications of using commercial data. I hope you had a chance to get your caffeine fix but I guarantee you won't need it because we have an exciting panel here and we'll keep it lively for you. We will probably stop for questions a little bit before the time that's in the program just to make sure that we have enough time to answer all the questions, and I would ask that even though we aren't the commercial data providers, the folks who didn't have a chance to get their questions answered in the first session, to please come forward so we can address your question. Can we just please introduce ourselves.

MR. PLESCO: Sure, can you all hear me without grabbing a microphone? For the record, I'll grab the microphone. Ron Plesco, I'm with SRA International. I'm Director of our Privacy Office of SRA.

PROF. SOLOVE: Daniel Solove, I'm a Law Professor at George Washington University Law School.

MR. GELLMAN: I'm Bob Gellman, I'm a Privacy Consultant here in Washington.

Mr. SCHWARTZ: I'm Ari Schwartz, I'm from the Center for Democracy and Technology.

MR. SPARAPANI: Tim Sparapani with the American Civil Liberties Union.

MR. VATIS: I'm Michael Vatis with Steptoe and Johnson in New York.

MR. REEDER: Good Morning, I'm Frank Reeder. I chair the Center for Internet Security and the NIST Information Security and Privacy Advisory Board.

MS. WITHNELL: And, I just want to note for the record that by my informal calculations what you see in front of you is at least three quarters of a century of experience in Privacy and Information Technology. So, I'm sure we'll learn a lot this morning. And that's just Frank Reeder.

MS. WITHNELL: We listened to a panel this morning that talked about the Government's use of commercial data, but one of the issues that I don't think we heard addressed was the wisdom of the Government's use of commercial data and whether or not it makes sense for us to be doing that. I thought we'd start this morning's discussion with Daniel Solove who will give us his overview of that issue.

PROF. SOLOVE: Well thank you very much for having me here. Can all of you hear me? Okay, well my part is going to be a little bit like rain on this data mining parade. What I think the primary attitude toward Government data miningg is this: Basically that data mining is really important to protect our security. It's a great tool, except it raises some privacy concerns and we should come with up some ways some guidelines to address the privacy concerns so that the Government can pursue data mining technology. I actually think this reasoning is flawed and it has two flawed

assumptions that I want to briefly highlight. The first flawed assumption is the assumption that data mining is good security. I'm not so sure that this is true. We face a number of risks in our lives; risks to our health, well-being, catastrophes such as we've seen tragically in the Gulf Coast and other things and one of the questions is how we should be spending our security dollars. How should we be spending our security resources?

One thing with data mining is we are still in the process of researching it and so a lot of money is being spent on technologies that are to some extent very speculative with benefits that are not proven, but that are somewhere down the horizon. When we have pressing national security concerns right here such as preparedness as we saw, at least in my estimation--, some might disagree -- but we were not very well prepared to deal with the catastrophe that struck us. We are not very prepared for an epidemic of bird flu or anything like that. There's a lot of things that our money could be going to and I really wonder whether data mining is a wise thing to be devoting so much time and attention to. I like it because I think it's interesting and I like talking about it, but maybe we shouldn't really be going down this road. There are security benefits that are much more immediate, much more proven, much more pressing than trying some data mining which is I think speculative.

I think one of the reasons why we're doing data mining is that after 9-11 there were a number of companies that went to the Government to dazzle them with the technology and the potential of technology and I think this got a number of people really excited about it, but I really don't think this is very good security until I'm really proven otherwise or until someone really comes forward and shows that okay, this actually worked. It worked really well. And it is a good thing due to the other risks we face. I don't really know this is the road we should be going down on. And the second assumption, which is related to the first is what I call, "Have your cake and eat it too," which is the idea that, well, we can come up with a good balance between data mining and privacy. I think there are certain things we can do better with data mining but I think that there are some trade-offs which even in the debates and among the people who offer guidelines, I don't see these trade-offs being addressed and I'm not sure they can be.

There are two types of data mining: there are actually many different types, but there are two types I want to talk about. One is known as subject based data mining; the other is pattern based. Subject based data mining is trying to collect data about identified suspects and I actually don't have much of a problem with this because this is very similar to what occurs in a modern law enforcement investigation. We want to find out more information about those of you we have identified as potential suspects. Pattern based data mining is different. This is like a dragnet search. It's gathering everybody's information and then seeing who fits a particular profile, and I think this is exactly what

the framers of our Constitution feared the most. Some questions that I just don't see being answered to my satisfaction in this regard are literally : why are certain people being singled out by data mining?. If people are denied something, will they have the right to a hearing? How long will it take for people to get a hearing? Do people have a right to an attorney? Will people be able to get erroneous data? How error prone is the data? What kind of system of accountability do you have if the data is not accurate enough but will be listed in t a report to the public? Suppose a person disagrees with the profile. Suppose a person says I don't like my profile. I don't think I should be on an extra screening list, or on a no- fly list? How can this be addressed at a hearing? And if someone says maybe your name doesn't match or whatever, you might try to get off that way. But suppose you're singled out as someone who is a security risk? Well, how do you get off of that list? Do you get to see the profile? Well no, in fact, one of the arguments behind the system is that we can't expose the profiles to the public because that -- then they're no longer a secret and then that tips off the terrorists. But if you don't expose them to the public how do you have accountability? How do you know people's free speech activity isn't in the profile? How do you know their free association isn't implicated or rights or anonymity?? We really don't. We can assume trust, but we really have very little mechanism for accountability.

So, it's really hard to raise a meaningful challenge as to what's appropriate and what's not in a profile if we really can't see the profile and if there are no transparencies there, and I don't know how you solve that problem. I really don't know how we get around that problem. I don't how you get around the basic problem of structure when it comes to this being a dragnet search. These are problems that I think no guidelines can easily and readily cure and I guess given the Pandora's Box this opens up is this really a road we want to go down? And the way we're going down this road is let's keep researching, let's keep planning, let's create all these programs, let's dump millions of dollars into this and then figure out how it's all going to work out in the end and assume that somehow we can balance it all out. And maybe we shouldn't be going down this road. The fact is, I don't know how good it is for security and it certainly has a lot of issues -- a Pandora's Box of issues with privacy -- and I don't see a lot of progress made in addressing those issues. So, I guess the thing I have to say is maybe don't do it. Data mining -- Pattern based data mining -- isn't working.

MS. WITHNELL: Would anyone else like to comment before I jump in?

MR. VATIS: Yes, I just want to thank Daniel because I wasn't really quite sure what I was going to say when I got up here. Now you're going to have to shut me up or throw something at me because I'm both astounded and perplexed by your comments. We just had a fantastic first panel where people with vast experience in these issues, both on the private sector side and on the Government side, told us about the very concrete,

very substantial benefits that they derived from data mining. We heard about how analysts and investigators can save tons of hours in re-sourcing and money that otherwise would be spent going around knocking on doors, looking throughhard copies of public records to find information, but data mining capabilities now cut all that short and allow them to devote their efforts and their time to other things, to doing the hard-core human analysis that's often needed for engaging in preventive efforts and the sorts of things that you say we should be spending more time on. Well, data mining allows us to do those other things that are necessary. So, I'm not sure what other benefits you're looking for if not the saving of resources so that we can devote our two-limbed resources to other very necessary tasks.

It seems to me that not only should we go down this road, but we're already well down that road and so what we should be thinking about is what rules and safeguards are necessary to protect the sort of privacy and perspectives you're concerned about and I agree with you, wholeheartedly, that not enough thought has been given to date to what those rules and safeguards should be. But that's precisely the purpose of this sort of gathering, to include what I hope are a series of hearings on the Hill, so that Congress takes up this issue in a wholesale fashion and not as I think Carol said on the last panel, in a piecemeal fashion, which is the state or the law today. You've got some isolated pockets of special protection for sometimes rather weird categories of information, like video rental records and the like, which were occasioned by specific instances in our history such as the Bork Hearings.

We need to deal with this in a much more comprehensive way to address the protection of privacy. We need to address things like what do you do with records that are inaccurate and that have consequences as a result for people's liberty interests or just for the way they lead their lives because they have to get searched every time they want to board a plane because they've got a name that might match somebody who is a real suspect but is not that person, yet they repeatedly get searched, such as one of the audience member's spouses, who raised this example during the break. So there's lots of issues that need to be addressed but we certainly should not just throw up our hands and say we shouldn't go down this road which, interestingly, was the initial take of people in Congress and I think in the media after the Terrorist Information Awareness Office came to life. It's interesting to me that in the year since then, that initial reaction has quietly subsided and agencies have continued to go about the business of data mining even though John Poindexter is not leading the DARPA office at the Department of Defense anymore . I think that development is a good thing. I think I have probably said more than I should have. I'll turn it over to somebody else. Let me just jump in.

MR. PLESCO: This is going to be fun because I think Mike and I are both supporters of TIA, CAPPS II and MATRIX. I'm just kidding. We ought to all go to lunch

now since we're all excited about it, but I understand, Dan, your points on subject-based searches. They've been done for a long time now by data mining or electronically. It does provide for efficiency in investigations for law enforcement and even the prosecution. Let's get over to pattern-based searches for a second. A lot has been written about pattern-based searches and a lot is misunderstood about pattern-based searches. The technology is based upon the profile, as Dan said. The profile is the key, a handful of clients and clients that are in current work environments where these clients who try to get to their arms around five to ten years in investigative data whether it's in the Financial Fraud Community or the Intelligence Community, or Law Enforcement Community and try to move that data into search algorithms based on [inaudible] MO's and crimes, this is was we see in our search data.

There is – I have great concern with those algorithms and the basis for them becoming public; however, I think there's a way to deal with this. I think the way is maybe from a judicial review standpoint. When I was a law enforcement officer doing investigations, I used that tool -- whether it is Lexis-Nexis or ChoicePoint -- and they used their algorithms to do their searches. At some point, some defense attorney has to challenge that and case law has to do be developed. What is the basis for that? Can Congress jump right now and point and give us some guidelines or maybe amend the USA Patriot Act, Section 215, to give 215 more teeth as some law review commentators have argued? Well, that might work, but the idea is to give some level of judicial review to that profile, the basis for that database search. I do agree with Dan, though, that this is all so new and that a lot of this began right after 9-11. A lot of companies went in and showed some of the technology and opened Pandora's Box, and it was accepted hook line and sinker by law enforcement and now we are just to dealing with how do we do that? At the end of the day, though, when you are dealing with investigations as the FBI said earlier, there are standards and Attorney General Guidelines that are employed. I think those have to be amended though by Congress. Thank you.

MS. WITHNELL: Anybody else?

MR. SOLOVE: Getting back to the debate here, it seems to me that a lot of the privacy invasive data mining and other techniques that are being used for security don't fail because they invade privacy, they fail because they don't pass the security laugh test. I think that many of these things are simply unproved for their security value. And I would like to ask a question and pose a challenge to the world, to the industry whatever, if all of this tracking of individuals, mining of data can be so effective to identify people who are terrorists, who are threats, who are criminals, then I'd like to know why an industry that has access to all of these tools and has lots of financial motivation to use them can't stamp it out or substantially reduce the amount of identity theft that is going on, much of which is perfectly obvious when you're the victim and you get that bill that

isn't yours. It's perfectly obvious that it doesn't match, that anyone who looked at it with any degree of acumen would recognize that the transaction that was engaged in was not done by the person to whom it's being attributed, yet none of these tools seem to be able to put a dent in the burgling identify theft, not to mention credit card fraud and all the other things that are costing industry and ultimately all of us a lot of money.

It seems to me that before we start using these techniques and even these behavioral kind of activities, trying to capture some type of predictions of what people are going to do next, that we ought to be able to prove these technologies in the realm identify theft would benefit us and then move from there to see whether the same techniques can be used in other harder areas.

MS. WITHNELL: I don't want to cut off the debate. Anybody else? We did hear this morning from the first panel about the benefits of using commercial data in various and similar ways and we are in fact embarked on programs that will ask us to use commercial data for purposes of identification so the next issue becomes does it make sense in terms of particular programs and in a more generic sense do we have the legal structures in place to serve as guidelines for the use of that commercial data? The Privacy Act that everybody has mentioned basically is the granddaddy of all privacy laws. It sets the stage for the Government's use of data, and I would argue that the Government's use of private sector data as well. The Privacy Act has a long history and I thought perhaps Frank, this morning, could give us a little bit of the flavor of that history so that we can see where we've been to know where we ought to be going.

MR. REEDER: And we have four hours for this. I realize that I'm guilty as charged about having a long history with the Privacy Act. As I've thought about this question and in the interest of the full disclosure Liz told me that she was going to ask me this question, I wasn't sure where to go with it but I guess I would offer the following: Around the time that the law was enacted, there were two things going on that I think were terribly important. One was the state of information practice, namely, we were coming off a period of American history involving distrust of Government's use of information and thus a political crisis as a result of which it became possible to get a consensus on a law that would place some restraints on Government 's information collection. I think most of us would agree that the Privacy Act is a disclosure statute really not a privacy statute. It requires agencies to disclose their information practices both to the individual with respect to a transaction and to the society as a whole through a variety of provisions.

The second is the state of technology -- I see a few of my colleagues in the audience. Some of us are old enough to remember what the state of technology was at that time. The state of technology was such that the kinds of data mining or even the ability to access data was rather constrained. It was pretty expensive even to search your own

database unless you had indexed it so that you knew what was in it. Hence we had a system of records concept in the Act that is largely irrelevant today. The system of records is a group of records that are retrieved by, not retrievable by, personal identifier. Computers back then didn't have the capacity easily to access information unless it was specifically indexed in advance. Accessing data that that had not been indexed could only be done at great cost and in fact, we didn't want to create or cause data mining to occur

The Act, again, didn't address important questions that I think the colloquy that you've been hearing so far has raised. One is obviously requiring agencies to disclose how they are doing things like using third party data for profiling, practices and technologies simply not contemplated by the Act. That would create the opportunity for challenges, which would in turn help to ensure that practices are not out of tune with what parties at interest perceived to be their legal rights and what is the appropriate role of Government. Then second, the Act didn't really address the cost benefit test. I hope that at some point in this conversation we deal with each of these important questions discretely. First, what is the legal basis for the practices that we're talking about? Second, - you can take the boy out of OMB but you can't take OMB out of the boy - What are the benefit cost implications; that is, is this a cost- effective application of technology, setting aside and assuming for a moment that it is a wise use of the data?

MR. GELLMAN: I want to disagree with Frank a little bit. I mostly agree with his analysis of the Privacy Act, but there are at least two substantive provisions of the law that have really attempted to impose real restrictions on agency conduct. One is the routine use language; the intent was to try to control how records could be disclosed. Essentially what happened is the over time subtle changes occurred in that provision, and it became a publication requirement. You can disclose a record for any purpose you want as long as you publish the right notice in the Federal Register, which is not what the law says.

Secondly, when the Computer Matching Act was passed, which was another amendment to the Privacy Act and another failed attempt to control use of information, there was an express cost effectiveness requirement in there. In order to do computer matching you had to show cost effectiveness and the agencies, aided and abetted by OMB, totally ignored the requirement and paid no attention to it and went on their merry way to initiate costly computer matching whether it made any sense or not. I think that was a very early attempt to control the same kinds of behaviors that we're talking about here on data mining and nobody wants to pay attention as to whether these kinds of activities are effective, are cost-effective, because it's too hard to show and agencies when confronted with that, simply will not –

MR. SCHWARTZ: Yes, I don't think there was too much of a disagreement there and I'm actually going to agree with both of you. In terms of looking at the Privacy Act

and what has happened to the Privacy Act over the years, you know Grace Mastalli from DHS said in the last panel that there's a lot of -- That the Privacy Act probably provided more flexibility than DHS uses. I'll probably agree with that based on the discussion that Frank talked about. Grace used the term flexibility. I'd probably use the term atrophy -- that the law has atrophied over the years because OMB wrote the guidance when Frank was there. Frank helped write the guidance 30 years ago, and the guidance, as a whole, has not been updated since. If you look at what DOJ prints out and try to read just the contractor clause, which is probably the most relevant clause for what we're concerned about here, there's a single paragraph on it and one relevant case on the provision. So, agencies don't have the kind of leadership that they need and GAO has continued to write reports stating this again and again. We still have not seen action to try to answer some of these questions that agencies desperately need. But in that case, it's up to the agency to step into the gap and make the decisions for themselves and DHS can certainly do that. I think there are some areas that are very clear. For example, when we talk about the Privacy Act, when a contractor is holding data for DHS and it's a new database that was created for DHS, the Privacy Act clearly applies. There shouldn't be a disagreement about that, although in some cases it seems as though agencies don't quite understand that today.

As a matter of policy, when a database is brought into the system -- into an agency, and it's the same database that's brought in -- clearly again, that's a database that's being used by the agency so you're taking a database that was held by some contractor and brought in creating a new database and that's a new system of records. I think that's pretty clear as well under the law, although some agencies have problems understanding that as well. The merger of information when new data is merged with an old system of records -- that, too, calls for a new system of records notice under the Privacy Act. Again, there shouldn't be that much confusion if you take new data and you merge it with something that is held by a contractor under section M, you need to have a system of record notice. Again, this is an area where there seems to be confusion, but there shouldn't be confusion about that. The one area where DHS should step up is in this question of what are the principles that should be put in place when a contractor holds information that is not specifically created for DHS, what happens in that situation? And OMB has not come up and said what should be done in that situation.

I was gratified to hear on the last panel that the panel seemed to agree particularly from Choice Point and Acxiom that Privacy Act principles should apply to the data that they hold that is used by the Government, and I think it is an important goal. I'll read a list of what I think the important principles are for Information Practice and Principles from the Privacy Act: To prevent the Government from creating secret systems of records, to make sure that people know that information exists out there, and to make sure that the Government is using that data appropriately -- that they make public the

collection and use of information. This are key principles. This is where I might disagree with Frank a little bit from what he said; it's not just a disclosure statute; in terms of principles, the Privacy Act sets out very clearly that you should only be collecting and using information for a particular purpose and you shouldn't have a use for all sorts of different purposes.

At least you should make it known what those uses are in advance. Ensuring data quality, information security, allowing correction, accounting for disclosures, those are all pieces that have been talked about earlier that are important. Training employees, again, is another important aspect that's clearly in the law and providing notice of exemptions in advance so that you know if you're going to use something for a different purpose that you make that known in advance. So, just sorting out those principles, we know what those principles are. DHS can make them apply to and should be working to make them apply to the contractors that they use in this circumstance.

MS. WITHNELL: Does anybody else want to comment?

MR. REEDER: Just a brief comment. The point that I was making was not so much the black letter law doesn't appear to place significant constraints on agency behavior, but the practical affect of those constraints has been negligible, to put it mildly, except information practices were enclosed largely through the routine use provision. I'll leave that to the lawyers of the panel to educate me, but I don't know of any instance where an agency's right to collect information has successfully been challenged and so as a practical matter, while the Act attempted to implement the code practices, I question p whether it has. So the question for me at this point in history without ignoring the very important questions that Dan has raised, is how do we create a regulatory or legal regime that requires agencies -- particularly other than the Department of Homeland Security -- that are not engageing in fair information practices to do so.?

MS. WITHNELL: Do you really think though that the Privacy Act is outmoded in that sense? It seems to me that it provides an overall structure by giving life to the Fair Information Practices for what agencies should be doing in terms of information collection and that one of the problems for the Privacy Act is that for years it was ignored by the world because information was not a big issue. Privacy and information security is now a big issue and everybody is looking to a statute that was put in place to give it some guidance on privacy, but for years and years people didn't not challenge it. Subsection M deals with contract information. It does, it seems to me, have a significant part to play in our use of commercial data. But I think there are three reported, or three cases, two of them which are not reported in the Federal Supplement that give guidance on the implementation or the interpretation of that provision. So to a certain extent I would say and throw it back to you, isn't there a failure on the part of the public advocacy groups or

others who have not taken this act to heart and basically challenged agencies when they saw they weren't doing what we were suppose to be doing?

PROF. SOLOVE: Well, the Act was born in a time when there was great concern over the use of data and the spread of data, as the HEW Report of 1973 notes. If you read that, which is the report that inspired a lot of the Privacy Act, it really does speak to our times. Part of the problem with the Privacy Act is it's not easy to enforce. Who sues or what do you get? I mean the incentives aren't there and it's incredibly hard and the Supreme Court has even now whittled away the liquidated damages provision. So, you have to show willful conduct to get your damages and then on top of that you have to show actual harm. Someone's social security number gets improperly leaked and if you can't show some kind of actual injury, which is very hard to do in these cases, you're out of luck.

So without the incentives to really waive the stick and make people pay, of course the Privacy Act isn't going to do much and people aren't going to use it. You have to give it teeth and the problem with the Privacy Act, it's almost like a guideline -- like be nice, be happy, do this and here are all kinds of different ways, such as routine uses, where you can fudge a little bit and because there's no teeth, there's no enforcement, meaningful enforcement. The problem i is if you really want to give the Act teeth, I think then you apply it to even negligent activity, I think that you really provide some very powerful whopping liquidated damages for violation so that people who violate this act know there's going to be hell to pay. But that's just not there in the Act so I think it's no surprise that we aren't seeing this enforcement happen in the Privacy Act.

MR. VATIS: I would submit that the Privacy Act is to privacy as the library provision of the Patriot Act is to libraries. That is it's almost completely irrelevant to the purported subject matter. The Library Act Provision of the Patriot Act actually has nothing to do with libraries. It talks about business records and tangible things. Sure it can be used to get information from libraries just like from any other business or organization, but I think to date, it hasn't actually been used to get information from libraries. In fact, the FBI has used national security letters to get information from libraries, not Section 215 to my knowledge.

And on the Privacy Act, I think as Frank said, it's really more about disclosure than about privacy. I think what we really need to focus on is the lack of substantive standards for determining when a government agency should be authorized to collect information from whatever source and use it for homeland security purposes, whether it's investigative, intelligence or protective in some fashion, such as being used by TSA to determine who gets to board an airplane and under what scrutiny. It's that collection point where I think that the most privacy is at stake, rather than how the Government maintains the records, what notice it puts out when it's going to establish a system of

records and things like that. It's that area of determining what substantive standards should apply to the collection in the first place where I think we are currently lacking standards and where they are most needed.

MR. PLESCO: Your point on the Privacy Act as to whether it is relevant or not. I agree more with Vatis. The Privacy Act or Subsection M is interesting. What does that notice actually get you? I agree with the discussion on the panel. It gets you the notice that DOJ and DHS are using this for investigatory purposes. Yeah, right, so now that you know that to get back to the question that was raised earlier, what is the effectiveness or use of that data? Did it actually work? how is it being used? From an operational standpoint, that is really my perspective. How are you using that data? How are my Intel groups using that? Can we get that data? What is it relevant to? Why is it relevant? That to me is the most important question. Sure, review the notices and I'm glad it's an educational plan. Our current clients and a lot of clients still ask, "When does the Privacy Act apply?" There's a huge educational deficit, the training needed l in federal agencies so that they can talk about the Act. They're utilizing data. We have those kinds of conversations with out clients and they go issue the notice. But operationally, who cares about the notice? That my question. You check that privacy box, you give them the notice, now operationally can you do your job or not? Are you on board just because you've given your notice. How are you doing that? What is that profile that you're basing that notice upon? And how does that profile meet with the guidelines, and are there guidelines for that profile? And a more important question, should there be guidelines? These are the questions that I think are relevant. We should have guidelines for utilization of personal information for data mining, whether it's subject based or data based search is working out.

MR. SCHWARTZ: I agree with that -- for the most part I hear that. I think there's one piece that -- I don't like to completely nuaa doing the notice and the transparency of the notice because that's where you say -- that's where you put forth the exemptions.

MR. PLESCO: Yeah,

MR. SCHWARTZ: That means you're making -- you're thinking about privacy in advance and that's really what's important about that provision and the Privacy Impact Provision in the E-Government Act as well. You know, it's trying to get that piece out in advance and open this key to fair information practice specifically for this reason. So, I don't want to minimize that part, but I also think laying out the principles as well in the Privacy Act how to put together kind of a road map for agencies that want to do the right thing, to do the right thing. So, we're not there yet where we have today a law in place that sets those protections out in a way that information is really protected but it still can flow, etc. But, we do have an outlook for framework for agencies to make the right decision.

MR. PLESCO: I agree. I think it's the education of the agencies on the framework. They go about and focus and they will come to the other side. The agencies that are doing the [inaudible] right I almost but are the ones all the way down to the operational point.

PROF. SOLOVE: Real quick point, and I don't know the agency that did this, but there was a privacy notice, for example, for some program collecting data on mothers and breast milk and all the privacy, all the exemptions in the Privacy Act are included which is typically how a lot of these things are done. It's just pro-forma to claim it all because you want as much possible future use as possible, which I think is a big problem. There are very little teeth to actually enforce a reasonably stated notice. Agencies can exempt themselves from parts of the Privacy Act too. So, it's almost, well if you want to be in the Privacy Act you can, but if you don't want to you don't have to be. The Act needs to have a little bit more teeth and it's basically almost relying on the good graces of agencies who are not malicious but who think why not put all the exemptions in when you can if there's no consequence to not doing it? Why not open it up? That's sort of what lawyers do. But you have to have teeth in this Act and until that happens I think you can educate, educate, educate, but I don't know in the end if that's going to be enough.

MR. SPARAPANI: I think Daniel's point is well taken. This is -- let's level with everyone here. The Privacy Act is a toothless old man. Its teeth are falling out. It has lost its dentures. It's virtually useless and all it does when it's taken seriously by an agency, is help them do sort of the baking in the privacy and that's very important certainly in the planning process, but it really doesn't affect what's going on today. We heard from the first panel, from Acxiom, that they are heavily regulated and they were operating in an environment that had lots of overlapping laws that made them control their own behavior. I think that's nonsense, and I think that's really where the discussion should go, recognizing that the Privacy Act doesn't have the kind of teeth that people talked about with the liquidated damages provision to the certain incentives that would cause people to litigate the Act. We end up in a situation where the Government recognizes that it does have to conform in some ways to the Privacy Act and therefore, just outsources its data mining function to a variety of commercial data broker companies. It literally does an end around – around the legal system -- and that's why we've had this enormous growth in the commercial data broker industry because it's virtually an unregulated industry when you look at it from a statutory standpoint.

Commercial companies can and do collect virtually any information they want and with only a few limitations, they can share it with the Government or sell it to other companies. So really what we need to think about is not really fixing the Privacy Act, because it does provide some good sort of baseline work for agencies that take it seriously, but really to think about what are we going to do with this enormous statutory gap that exists? That is, you know, into which agencies that want to gather information

are rushing and they're doing so because they're contracting around their own legal restrictions.

MS. WITHNELL: It seems to me this is a good point that we can then ask what should we be doing if not amending the Privacy Act, what would you suggest in terms of a statutory framework?

MR. SPARAPANI: I don't want to seize the floor here, but, you know, my thought is this, companies who co-modify data, that's the situation that we're in right now. You've chosen something that you can buy and sell. You asked for it, you deserve the responsibilities that you should get from that co-modification. I think they flow from taking other people's information and selling it and making a profit from it and those responsibilities grow by an order of magnitude when you choose to engage in law enforcement operations and homeland security operations. You have a manifold responsibility to the public and to the Government to do more than you have done and to do more than simply the law requires, which is, as I said virtually nothing, so I would advocate for the mandatory application of government contract penalties to companies that are engaging in a contract with homeland security functions so that when those companies have a breach of their data -- when their data is either hacked or they lose it -- there should be some penalty. The Government should demand some sort of pecuniary return of the contract amount that was paid to that company. There should be a debarment. There should be suspension when there's a repeat violation because you hold the public's trust, because you're the first line of defense as conceded by a couple of the agencies this morning. You have to do more and the penalties for your failure should be higher.

MR. GELLMAN: What do you do about all of this? All the problems of the Privacy Act? What are the limitations in the Privacy Act and the simplicity in a way of confining the Privacy Act? Not all agencies are doing it. They're simply ignoring their actions or they're not doing it well. There's no oversight [inaudible] in the system, as Dan said, there is no teeth. If you have a system of records that is all positive with exemptions. You can claim every exemption under the Act. There is no one to say, "Wait a minute -- you really need that exemption?" I'll give you some specific examples here. If you have a system that is subject to one of the general exemptions, you can exempt yourself from the requirement of the law that you be held accountable -- that you can be sued. Now, I think that is really a poor judgment on the part of Congress to allow that to be done, but there are some agencies that say, "Even though we can exempt ourselves from being held accountable, we're not going to do it. We're going to use exemptions selectively and we will remain accountable for our actions because we think it's the right thing to do."

One of the newer techniques to try to put some teeth into the system is the Privacy Impact Assessment (PIA). The problem with PIAs -- and this is all Congress's fault -- if

you look at the requirements, there's no "A" in the PIA. There's no requirement that you assess privacy. All there is, is another requirement to describe what you're doing and while some agencies seem to be doing a good job with PIA's, many of them are simply taking descriptions, publishing them or not as the case may be. It doesn't have any impact on them. It's just check in the box to show what you're doing. My solution to all of this, and it's not the only solution by any means, is something I've been harping on for a very long time: we need a privacy agency in this country. We need a independent regulatory federal privacy agency that can serve to focus attention on the engine the system and can go back to an agency and say, "Wait a minute, you're not doing this right, you're not doing this well, you haven't considered something." Under the Privacy Act, that function basically falls on OMB, which passes on it and basically can't do it. We need somebody dedicated to this. There are CPO's in agencies and they can be useful in this way, but they don't have the independence that you require. If we had an independent private agency -- and I might point out for those of you who don't know it, that virtually every other industrialized country around the world has a privacy agency --. If we had an independent privacy agency, a lot of what we are doing right now would work better simply because we would have attention paid to the system and would be able to hold an agency more accountable in the decision-making process for what they're doing.

MR. SCHWARTZ: I don't want to take a step back from what Bob said, but I do think there are a few different issues involved here. The problem that Tim was talking about with Government using the private sector to skirt some responsibility from the Privacy Act exists -- We can get at that through various ways. I mean DHS can write its own rules today to get into the spirit of the Privacy Act for the use of that information and it would follow under the Privacy Act or the internal policy on how to deal with the Privacy Act and we encourage DHS to do that today. So, there's not the limitation that you have to go to Congress to implement the law the way it should implemented today. Could we do it? It's guidance on this particular issue at large.

That's another thing that could happen. Make OMB take on the responsibility that they should have had over the past 30 years to redo their guidelines and have not done. So there are things that can be done today to address that particular problem involved there. The larger question of some of the holes in the Privacy Act I think that's kind of a long return – larger discussion. I don't want to get too far off some of the commercial -- the specific commercial data issues. But, you know, there are some -- I'm just saying there are some steps that can be taken today without Congress acting, although certainly we've been pushing as part of the data broker bills to include Government provision of Government use in there. The Specter Bill does that. We think that's a great starting discussion point and we should use that as a launching point to have a further debate on it.

MR. REEDER: I must confess I deeply believe that the guidelines that we wrote in 1975 are still seeking this revealed truth. We're getting over it. I think that's absolutely right for all of the reasons that we discussed. I think we need to make the distinction between agencies having the ability to do the right thing, which I think we seem to agree that they do, and whether there is a requirement and further, not only a requirement, but an effective enforcement mechanism to make that requirement real as opposed to yearly purgatory. We would act among other things and that states a principal of information collected about individuals that would be used to make determinations about them, ought to be collected from the data subject to the maximum extent possible. As I said, that last phrase obviously is a huge hole through which convoys of trucks can and have been driven. But the spirit certainly suggests that individuals ought to be on notice as to how information about them is being used, and not through third party use suddenly find themselves adversely effected. While I'm sympathetic to Tim's notion that we ought to legislate the large question and would love to be party to that, I think in the short term we can come at it the other way and that is at least begin to require -- not nearly permit -- but require that agencies be good [inaudible] especially taken with Ari's typology.

If you look at section M, the provision that deals with contractor information, or information that's used by contractors. There's a huge hole. And that's the use by agency of information that continues to be maintained by third parties. I fully expect and hope that perhaps as a consequence of this workshop and through the DHS's own Privacy Office, that DHS will address this issue, I'm not equally confident that others will, and at a minimum we need to address that, and in the process I think there are other fixes we need to make as well. It may not be practical to require agencies to begin to become the first collector of information. But to the extent that use of third party data passes legal and benefit costs or cost effectiveness tests, certainly there ought to be much more stringent requirements that implement provisions of notice among others for those uses of third party data.

MR. SCHWARTZ: Can I just defend the privacy impact assessments real quick since no one else on this panel probably will. First of all, I want to get at Sarah's comment. Sarah asked this question to the last panel:, How can this work. How can privacy impact assessments work, if the environment is changing? That's exactly the way the law was set up. I mean part of what Bob is complaining about is the flexibility of the way that the privacy impact assessments are set up. It specifically allows people not to just publish in the Federal Register, but to publish it on their websites, so that it can be updated regularly. It also says specifically that National Security and law enforcement PIAs don't need to be made public. So it would depend on the particular situation. They need to be done, but they don't need to be made public. So they could be accessed to see if something went wrong, how the assessment was done, what the thought process was I agree with Bob that some agencies do look at it like a check box and that is a problem with

it. It was watered down from the original discussions that were had in the early versions of the drafting of the E-Government act. But certainly if you look at the history of security, and security provisions within the government and how they have increased over time, at first government had to make a statement about its security. And then it had to be certified, and then it had to be audited. And so now we've been strengthening those --that original idea of writing that statement.

We see the same thing happening in privacy as well. The problem that we have is that we have DHS and the Postal Service and maybe a couple of other agencies that have done really just excellent jobs in terms of drafting PIAs and putting them together and treating them seriously. And then we have these -- we have people who aren't doing it at all, and it hasn't really been called out until recent GAO reports that Chuck talked about. The PIAs that are done really poorly. That are just one page descriptions rather than going into the details, addressing all the points that they're supposed to address under the law. So it is up to Congress to oversee that. It's up to the advocates to say that this is not good enough from an agencies that are not doing a good enough job. And it's up to OMB to put out kind of best practices for drafting PIAs just so that agencies have to live up to a certain standard in the PIA. And that's the way we're going to be able to get to the point of saying well now that they're up to this certain level, we can actually certify them. We can actually start doing audits on certain ones that are very important.

MR. SPARAPANI: I'd like to respond just briefly, not to Ari's point but to the point Frank made before that. I don't think we can just contract this away -- in terms of the language and the procurement that agencies are making. And the reason for that is because most of the contracts in the Homeland Security context are sole source contracts. And they are contracts that take an enormous amount of investment from the companies. But what that means is, is if a company fails to secure its data, fails to perform the National Security function that it's offering to perform, the government just simply can't walk away from that particular vendor, particularly when it's a critical function. There's no other company that can immediately step in, take over the software, take over the function. It takes years to implement most of these programs, as was seen since 9-11. A lot of the times -- you know a lot of the programs that were proposed in the immediate aftermath of 9-11 still aren't up and running and that's largely because their very difficult to do. But what that means is when a company fails there isn't another company that immediately can step into the void.

So I think we need to have an acknowledgment before the actual government contract is written that regulates behavior, that changes and guides the behavior of these companies, that tells agencies we will apply some sort of punishment. We will slap the hand of the company that is failing to secure its data, that fails to provide you with

accurate data, that fails to audit its data, and I think these three problems are paramount in this area.

MS. WITHNELL: Are you saying that contractually we should make sure that the company with whom we're contracting has adequate security in place? I mean I understand the rationale. But I feel like if there is a data breach from a data aggregator, that's one issue. But the separate issue, and I think it's a separate issue, is whether or not we should be contracting with this company in the first place. And if we are, how we should be using that information. So to some extent I feel if we include these provisions in the contracts, a, we might scare them away when we need their information, and b, it's more or less to me apples and oranges. Our use of the data is separate from their breach problem.

PROF. SOLOVE: Well I think that one of the things we need is an understanding before we engage in it because you can't think about privacy after the fact. We need to ask, That is the use of the data effective, is a particular use effective? F, Is it even consistent with our basic constitutional structure? And can it be carried out in such a way, and sometimes I wonder, if you have the use of profiles that are secret and then you want judicial review how do you have that? How do you allow people to challenge something if you're not going to reveal to them what it is they're supposed to be challenging? Judicial process is supposed to be open, so how do you have a closed judicial process? How is it consistent with the very strong tradition, the bed rock principle in our country against dragnet searches?. I think you need to think about all this before we start going down this road Wouldn't it be cool if we actually put cameras in everybody's home? Wouldn't it be cool to strip search everyone at the subway? I mean a lot of things would be interesting and could have benefits too, but they're just non starters because there are so many difficulties in fitting them into our current regime. And I think that we need to think about different kinds of uses of data.

And there are different kinds of data mining, some of which I think are compatible with our system, like subject matter data mining, or subject based I really haven't seen a way that we can fit pattern based data mining into our constitutional structure, and I think that it's great for Amazon to market a book for me based on it. I mean great. But that's a different thing. That's marketing a book to me. It's really different in determining whether or not I get to fly on a plane. Or who is singled out on a naughty list or a nice list. And I think we need to think about whether we want to go down that road, do we want to explore that?. I'm not saying that data mining is inherently dangerous. It's good for some uses -- for commercial uses. We don't care how accurate it is. So what if they recommend the wrong book to me. It's very different when we're talking about who gets to fly and who doesn't get to fly. So I think we need to really think about what kinds of uses of data should we be vigorously exploring and what kinds of uses of data shouldn't

we. And with data mining, there is some kind of data mining we should go forward on and some kinds that maybe we should hold off and put our energies into the ones that we know are compatible with our system. And that work.

MR. REEDER: This is a terrific conversation because it's forcing me to think. I've heard two different questions that perhaps at some point become the basis for conversation. One goes to the purpose of the data mining, which I would argue is an appropriate subject for this conversation. And I'm not sure that there's anything inherently sensitive from a security perspective in talking about whether or not data mining is cost effective and constitutionally or legally appropriate for example to screen people who are getting airplanes. I mean you could have that conversation. It may very well be that having said yes, it is appropriate, it isn't appropriate then to have a public conversation about the particular profile that may be used, and we need to start thinking about procedural mechanisms where that issue can be joined, but really then it needs to be a two-part question. And I would hope that out of this conversation, and I think this is occurring, because it certainly occurred, for example, in the way the Department handled things like the USA VISIT program. It doesn't get into the details of the security features of the system, which are legitimately sensitive.

So I would urge that we parse what is an appropriate question into those two pieces. That is, whether the general use is compatible with our legal system and cost effective and that we force ourselves through a process, and I think USA VISIT is a wonderful example. I'm fond of finding things that actually have been done well. And I think that's a wonderful example of the Department having gotten it right. And I encourage that conversation at the appropriate [inaudible] of the process.

AUDIENCE: I'm Dane Von Breichenovchardt with the United States Bill of Rights Foundation. Thank you. I will make this short. I was wondering if you all comment on two aspects of 9-11. Do you feel that 9-11 in a sense has given a a de facto probable cause to law enforcement agencies, Federal and otherwise? That because we now have terrorists and we've been attacked, you should lower the bar and we kind of have a general probable cause, we ought to be able to go and look at anything anytime, under the auspices of the protection that we're trying to defend the country? And the second one is, had it also caused the general public to sort of become inured to just accepting these intrusions into our life that we're losing our sensitivity at both ends, the probable cause concerns and the citizens tolerating this sort of thing?

MR. VATIS: If no one else wants, I'll jump in and give you my answer to your questions. I think on the first question the answer is no. I don't think that law enforcement now operates under the benefit of some sort of generalized probable cause, where they can go and do whatever they want. They have to show probable cause if they want to get a search warrant or some sort of wiretap, there is still a judge who needs to

review the evidence that they proffered to see if they've met the legal threshold. Now do judges operate in the realm of everyday life where they're affected by circumstances? Yes. But I think, despite that sort of recognition of reality. they still apply the same legal standards and law enforcement has to meet those standards. On the second question, I think there has been a lot more willingness of the public to accept government activities that might not have been so acceptable before 9-11. But I think at least in the last year, we've begun to see the pendulum start to swing back. The attention to identify theft has been remarkable to me. It's gotten to the point where I think it's actually been quite overplayed. I was getting a ride into the city this morning, I was listening to NPR and I heard a story about what victims of Hurricane Katrina should do to prevent themselves from becoming victims of identity theft, because they had to vacate their homes, and they left credit cards records and things. They need to be worried about their identities being stolen. And I was thinking well this is quite remarkable. I think those people have a few other things of higher priority. This was NPR; this wasn't FOX news or anything like that. But nevertheless there is more and more attention now paid to privacy and I think that's a good thing. I wish we could keep a more steady level of attention to the important things rather than have it swing in response to events. But that's reality.

MR. REEDER: I defer to the distinguished legal minds on this panel to answer the first question. But to the second I would only add, I don't know, not having taken the pulse of the American public, where they are at any particular time. But I would submit that for at least in my experience, privacy and what is an appropriate protection is very individual. And whatever regime we develop needs to acknowledge and -- I steal a wonderful metaphor that I hear Ari use from time to time. Some of us are willing to give up a great deal of privacy because of the perception that it somehow makes us safer or as a matter of convenience. And I love what Ari said. Some of us have -- would love to have single identity for all purposes. Other of us compartmentalize our identity and carry multiple keys because we're not interested in giving people access to everything, and willing to bear that inconvenience.

So whatever regime we come up with apart from whether there is some prevailing swing in the public sentiment in one direction or another, we need to recognize that for some of us, the ability to be very private in those aspects of our lives that are none of anybody else's business is far more important than we're even willing to admit. We bear a great deal of inconvenience like you know paying cash at the Safeway and foregoing the ability of Safeway to profile who we are, or perhaps there is some sort of little optional scheme under which we can be pre-cleared to get through security more quickly in airports. Some of us will be willing to do that, and others will not. So whatever we come up needs to recognize an individuality that's inherent at least from [inaudible] the notion of personal privacy.

PROF. SOLOVE: Very briefly on the second question, I think yes, I think there was at least initially a sentiment and a belief that we want more security. And the sense that I often got is that if we give up privacy, you're suddenly magically going to get security. If something seems really invasive, people think, "Oh that has to provide more security." And I do hope that, the government officials realize that people are afraid. And when people are afraid that's when they're not likely to think as sort of rationally and really assess the risks and the costs and the benefits, and that's what government's supposed to do. It's supposed to be sort of wiser in these times and less reactionary. Because we have - the risks that we face are infinite. The amount of target - just from terrorism there's an infinite number of risks, there's risks of [inaudible]. There are risks of all kinds of things that we face. And I think that we need to think about - we only have a finite number of resources. And what do we do?

So the reaction after the London Subway bombings was for New York to create a system where they searched the New York subway riders. Well there's like 4 million subway riders a day in New York. It's ridiculous to think that that's actually going to provide a lot of security. It made people feel better. You'd hear people say, "Well, I feel I am more secure because I was inconvenienced today." And I think these look great, they're symbolic, it looks like you're doing something and then you can say, "Well, see, we did something. But it's not really a good expenditure of time and money, and resources. Police officers have to do these searches. I think that's a waste of time. It's taking money and it's throwing it down the toilet. You get less security, in the end because we're exposing other targets and all we get is that people feel better. And I guess the question is, to what extent should we take measures to make people feel better, even if they don't work very well.

And sometimes the most effective things don't make us feel more secure. But they might be actually the most effective security measures that we can take. And they're often sometimes simple, like we go abroad and really try to lock down the loose nukes. People don't really experience that, because they don't see it day to day. So they don't think "Oh, the government's really doing something." But that might actually be the most effective thing that could really avert a horrible catastrophe. And so part of it is doing the hard work, which is not giving into the fears of the moment and really thinking about what are the risks, what are the things that we should keep doing and not get derailed over trying to do some kind of symbolic thing to protect privacy.

AUDIENCE: Could I refine the first part of my question. Because I think, probably, I didn't use the best words when I said about a de facto probable cause. Let me put it another way. Under the Patriot Act, they go before the FISA court, they've lowered the bar to simply you know, they don't have to go in with any probable cause to get a search warrant, they just simply say that it relates to an investigation of things. We had an FBI

agent here earlier who talked about -- first of all we all know the FBI used to only go into acting prophylacticly -- they go out and try and catch things before they happen. Which is fine. But what you have to understand is that one of the points that he made is that what triggers an investigation; we've gone from probable cause to reasonable suspicion, and it keeps dropping, and dropping, and dropping. And what I'm saying is are we trending towards a way from hard probable cause before law enforcement sticks its nose into our business to a lesser bar of sort of a merely curious standard. And you know, I'm exaggerating , but are we being inured into accepting a lower standard of curiosity for law enforcement.

MR. SPARAPANI: I'm not sure I can respond directly to what law enforcement agents are thinking. But I will point out that this is an important cultural moment, and shouldn't pass without sufficient comment, scrutiny, and discussion in the public. Our constitutional norms are threatened at moments when the country feels a threat. It's not a new thing. It's a cyclical thing it's happening again. And we need to just pause and at least consider whether or not by changing our cultural structure we are giving the terrorists the very first victory. I mean by changing our culture. It's a broader question than this panel is designed to ask, but it's the basis for a lot of the programs that are in place here.

As to whether or not people are inured to giving up their privacy, I think the answer is certainly we are all becoming more accustomed to that. And this is largely because in the last several years we've taken a turn towards identity based, or identification based security as opposed to physical security. One of the things we've touched on and Michael mentioned is this problem of identity theft. And I think it is the Achilles heel of much of the security, the layered security apparatus that the various governmental agencies have put in place. And that is because it is an identity based system that we are using to identify who are the bad actors in our society, or who may be moving amongst us. And it is remarkably easy as we know it to obtain somebody else's identity and assume their identity. We have designed a system with these fatal flaws. And I want to point that out before we move on.

PROF. SOLOVE: One quick point in response to your probable cause. I actually think that there's this -- I think the culture changed a bit after 9-11, in terms of the law, I mean the Patriot Act does do certain changes, but the standards, reasonable suspicion, the criminal standards, all were in place before then. National Security letters were in place beforehand. So there's this big dance about Patriot Act Section 215-- oh it doesn't apply to libraries; it does; it's not that bad; it is that bad. Well the big issue is you have National Security letters too. And so its not just 215 it's not just security letters, you wipe out the Patriot Act, you still have problems and that's because there are problems that pre- existed the Patriot Act, pre-existing 9-11. The Patriot Act came in and basically I see it as pouring

salt into an open wound. And it just exacerbated a lot of things, but getting rid of the Patriot Act doesn't get rid of the wound. It just gets rid of the salt. And the standards were put in place, there are number of I think very short-sighted Supreme Court decisions, laws that have loopholes that require lower standards. It goes back to the wire tapping laws, electronic communication privacy act, where the original NSL provisions were in place, so all that FISA has -- and all this is pre-existing.

So it's not suddenly in 2001 our law suddenly dramatically changed. It's just that the culture changed. I think that the Patriot Act poured a little salt in these wounds, but these wounds have been festering for a while. And I think that now people are beginning to see them. And see what's happening. This is something that's happened over the past 30 or 40 years with the Fourth Amendment being whittled down with the number of exceptions, with a series of statutes filling that void, that are not very protective. So I think that's sort of the picture. But it's not something that certainly magically happened three or four years ago. It's something that had already been in place.

AUDIENCE: Good afternoon, my name is Jason Kerben from the Department of State. The Federal Information Security Management Act requires a number of specific security controls to be placed upon -- and those are management, technical and operational for executive agencies. And also for any third parties, that do work on behalf of those executive agencies. There are a number of special publications that spell out those security controls, and provide guidance to executive agencies how to implement that. Does that, and my question, I'd like Mr. Reeder to start off by answering. Do you see that as the teeth, or some level of enforcement that could be applied upon these data mining companies that are providing information to government agencies with respect to the Privacy Act.

MR. REEDER: Well I think the short answer to that question is to the extent the activities of those entities are reached by the Federal Information Security Management Act, we have the same enforcement problem. Only worse. I mean the penalty for failing to comply with the Federal Information Security Management Act, is a yellow and a red, rather than a green on the President's management report card for the agency, on behalf of the contractors operating systems. I don't know of any other penalty provisions.

MR. SCHWARTZ: You can get an F from Chairman Davis; he'll give you an F.

MR. REEDER: Yes, I'm sorry. And you know these stories have extremely short legs as they are communicated. Some are usually on the Federal page of the Washington Post, not read by many, just those of us that live inside the beltway. So as a practical matter, as I look at the challenge generally, not just with respect to third parties who operate systems on behalf of agencies. In fact, most systems are now operated by third

parties. [inaudible]. The penalties are meaningless, under the FISMA in my view. On a completely different subject, but one I care somewhat passionately about, there is a need for creating an incentive structure for security, for effective compliance, but I'm not sure that the legal remedy is the appropriate solution.

MR. SCHWARTZ: I would say that with FISMA that it is the same problem right, because you still have the incentive problem that we were talking about with the Privacy Act. FISMA was passed as part of the E-Government Act. The Privacy Impact Assessment piece was passed as part of the E-Government Act. I would say a lot more resources are being put towards FISMA right now. And I think that's different from what I was saying earlier, because I think FISMA was changed over time First it was GISRA or whatever the past version of - it was originally Clinger Cohen, right?. But then you had more changes -- and what FISMA did was change to certification and audits. And I do see that as kind of the next step of -- am I mischaracterizing this Frank? In terms of the focus towards security and outside security FISMA is moving toward increased security and the movement of privacy should be in the same direction. They both are not perfect right now, and both need some work.

MR. PLESCO: Just one more point on that issue. Two clients that come to mind that see privacy and security as the same though with different drivers. And you have FISMA driving them on the certification and accreditation side but do not impact in our project usually. They're actually now pushing off to their third party providers or network hosting companies that they must be FISMA compliant. Now the interesting part is that we have two cases, a gentlemen in the front row, and I had to write an opinion on this for one of these companies, or with one of these Federal agencies. We also use SOX, Sarbanes Oxley, and this is a SOX company that has internal audit controls and security and used that as a motivator. The private sector company, is pushing back to the government agencies that they didn't have to be FISMA compliant. That they just collected all this data, but FISMA didn't apply to them. Well, you know, thank goodness for [inaudible] who sat back and said, "Well we don't have to do business with you." So they're forcing them down the FISMA route. But also that [inaudible] also went up to the manager of the company to let that company's CPO and CIO know that they have issues. And since they have issues they also have SOX issues. And wouldn't that be great [inaudible] use that [inaudible] layout that.

MR. REEDER: I only add one sentence because I said there's a risk of turning this into a conversation about FISMA, which it is not. And that is I would simply point out that the assumption to having an accredited system doesn't have anything to do with security. [Laughter]