

>>Yael WEINMAN

Welcome back, everyone. I think we would all agree that the first panel ably moderated by Hugh Stevenson really set the stage for us today. So thank you to all the panelists from the first session. We have six panelists here this morning with us. They are all going to present a different angle on setting the stage for the laws that are currently in place relating to data security requirements. As you all know, or if you don't know, I'll let you know now, the data security laws that the FTC enforces, including the general Section 5 FTC Act, laws in GLB, the safeguard rules, laws relating to the Fair Credit Reporting Act provide a general standard of reasonable safeguards. Some would call it vague, some would call it general. I'll let you decide and that's something we can explore a little bit more throughout the next day and a half. Our first speaker will be Jeffrey Kopchik from the FDIC and he'll give us a general overview what financial institutions in the United States have to deal with in complying with the various data security requirements that his agency enforces. Next, we'll hear from Peter McLaughlin, who will talk a little bit about the states, which we've heard, have some more specified requirements, and there may be some challenges to organizations in complying with both the Federal requirements, requirements of the states, and we have Chris Kuner, who will give us the overview in Europe.

He's the chairman of the International Chamber of Commerce Task Force on these issues and he's also a partner at Hunton & Williams. Next to Chris we have Sophie Nerbonne from the French Data Protection Authority, the CNIL. And next to Sophie we have Yoram Hacoen who is from the Israel Data Protection Authority. -- I didn't -- Yukiko Ko from Transunion, who is one of our company representatives here today to talk a little bit about industry challenges and complying with all of these requirements. And finally, Yoram Hacoen from Israel, representing the newest country with data security requirements. And so that's going to be the general overview. Before we begin I want to make mention of an article that I clipped over the weekend from the "New York Times" that discusses the surge of bank robberies in New York City. As you'll see, banks not only in data security requirements online but also data security requirements -- physical data security requirements within banks. And Raymond Kelly, who is currently the police commissioner, has a long, esteemed career in New York City, is looking for some specific guidelines that banks need to comply with in dealing with physical security, and the New York Bankers Association is resisting this, and I'll quote what the current president of the New York banker association said. He said he would prefer that banks tailor their own security plans rather than have blanket directives

hoisted upon them by law. This quote really struck me over the weekend as we sit here and begin to discuss these issues because they are not very different from physical security issues. So with that I'm going to turn the mic over to Jeff who is going to give us an overview on financial institutions and what requirements they have to deal with. Intermixed between speakers we may have some questions we can take or I might ask a question that might seem appropriate. Jeff.

>>JEFFREY M. KOPCHIK

Thank you Yael. For those who are here for the first panel, I would like to thank Marty and everyone else for saying that I think they set up my remarks perfectly. So in terms of giving a very good lead-in to what I want to talk about in terms of data security statutes and regulations in the United States. I think that most of you know that from my perspective, the United States really doesn't have, as other nations do, sort of an overarching data security law. What we have are multiple laws that tend to be sector specific or what I refer to sometimes as issue specific. So my remarks as Yael indicated, we're going to talk about the two primary Federal statutes that deal with data security and the implementing of regulations that the banking agencies put out to basically make those statutes effective. The two laws I'm going to be talking about are the Gramm-Leach-Bliley Act

of 1999, which is commonly referred to as GLBA in the United States, and the Fair Accurate Credit Transactions Act of 2003, which is commonly referred to as FACTA. Both of these were basically effectuated by implementing regulations. In the case of GLBA, some supervisory guidance that the agencies issued. Banking agencies do a lot in the United States at least of their most important work through guidance. So if you want to look to see what is a bank regulator's position on something, you can always go and look at the regulation but you would immediately follow up and see if there is any informal supervisory guidance about that. Let's talk about GLBA first. Section 504 B of GLBA requires the Federal banking agencies and also the Federal Trade Commission and the Securities and Exchange Commission to promulgate regulations establishing standards for safeguarding customer information. And just as an aside, customer information in this context refers to consumer information. It does not refer to business information. The guidelines that we promulgated became effective in 2001 and what they require is that the institution do a risk assessment and then put together a comprehensive written information security program to basically ensure the confidentiality and security of customer information. Now, on the first panel they talked about, if you read the guidelines carefully, you will note that they do not specify

any particular type of security control. What we're looking for is this overarching program. The guidelines, however, do go on to say that in the context of putting that program together, that the financial institution has to consider eight specific type of security controls, none of which will surprise you. For example, we're talking about logical and physical access controls, the use of encryption. Intrusion detection systems. Response programs. Dual controls on data and access to data. Change controls procedures. Business continuity planning. What happens if there is a hurricane and your data center gets destroyed, that sort of thing. Keep in mind that what the guidelines require is that the financial institution consider those eight and adopt the ones that it feels is appropriate to its specific type of business. And that group of eight is not exclusive to the extent that there are other controls that don't fit into these categories that may be relevant to the financial institution. The examiner would expect that the institution would institute those controls also. The last thing I would like to say about the GLBA regulation, which is also relevant to what the first panel talked about, it contains a very specific requirement that says that the institution is obligated to basically update that plan as necessary going along. So what was promulgated last year in terms of an adequate data security protection program may not be

appropriate next year, and the institution just can't sit with the program it initially implemented and never go back and amend it and change it. One, as the threats change, and secondly as the business arrangements that the financial institution is engaged in change. Now, as I mentioned, in the case of GLBA, there were 2 pieces of basically supervisory guidance that the agencies issued that basically flesh out and interpret the regulation. The first one has to do with customer notice. In 2005, what the banking agency said was, we interpret the GLBA guidelines to say, if there is a breach of sensitive customer information and misuse of that data either has occurred or is reasonably possible, then the institution has an obligation as we see it to notify the affected consumers. They only have to notify the affected consumers if the data has been misused or reasonably possible and it gets to the question of the background noise that the other panel was talking about. We made the judgment, we don't want notice in all cases, but they have to notify their primary Federal regulator in all cases of the breach and that's really the check. Where the regulator can sit there, we can look at it, and if they chose not to notify consumers, and we feel that that was an inaccurate interpretation of the guidance then we can talk to them about that and prompt them to say, no, in this case, we think the customer notice may, in fact be appropriate. I

just want to point that out. The other piece of guidance we issued in 2005 had to do with stronger authentication and this goes to the security requirement and access controls, where we made a determination at that time that most online banking systems that gave consumers and businesses access to money or access to personal information, the only thing you needed to get on the system was an ID and password and we came to the conclusion at this point in time that was no longer adequate for what we deem high-risk systems. Again, high-risk systems are, you can access sensitive personal information or you can transfer money out of the bank. So what this guidance says, if you're a bank and you maintain that type of system you have to have an access control that is commensurate to the degree of risk and is stronger than an ID and a password. Again what we didn't say was, what precise type of technology or technique do you have to use. We said it has to be something at least one notch up from the I.D. and password. And if you look at the appendix of the guidance there is a long explanation and description of what the agencies go through for various types of authentication technologies available. Multi-factor authentication using tokens, that sort of thing. We give some hints as to the type of thing we would like the banks to consider. But again, no specific technology is required. Let's move on to FACTA. There were really two sections of

FACTA that resulted in specific regulations. Section 114 of FACTA required the Federal banking agencies and the Federal Trade Commission to promulgate regulations that require financial institutions to implement a written identity theft prevention program. Now, from my perspective, that is actually broader than the GLBA information security guidelines, because really, while a good information security program, I think, is inextricably linked to the idea of helping to prevent identity theft, there are other things you probably can and should do to help prevent identity theft so this regulation said to the financial institutions, again, you have to put a written program together that the bank examiners will look at. But once again, the regulators did not tell the banks how to do it and we had a similar requirement that said you have to basically make sure this is updated on a periodic basis. The second regulation I'll mention very quickly is section 216 of FACTA that said that banks have to have an appropriate and proper way of disposing of consumer information so it doesn't end up resulting in identity theft. Now, what are the 4 points that I would like to make, sort of general, in each of these cases the banking regulators did not require the use of specific technologies or techniques that could come, from our point of view, out dated. We took what we refer to as the accountability-based approach where we set

forth certain objectives that need to be accomplished but we let the banks basically work with us to figure out the best way to do it. We think that the two advantages of this is, one, it eliminates the need for the regulators to go back and keep rewriting the regulations to take into account changes in threats or changes in business. It gives the institutions the flexibility to sort of try various ways to reach these goals, and for us to then sit there and also learn from what they are doing to see what approach we think works the best and makes the most sense, and we can sort of carry that further. So that's it for my introductory remarks.

>>Yael WEINMAN

Thanks Jeff. I'm going to pose a few follow up questions based on what you discussed. One, what legal effect does guidance have? Secondly, who did you consult in developing this guidance? Is this the kind of thing where you had an opportunity to participate in the developing of a guidance? Have you modified guidance since these laws went into effect? Is industry clammering for changes at this point?

>>JEFFREY KOPCHIK

That's four. Do I get all four? I can maybe have three, and after that, you'll have to remind me. With regard to the first one, basically, the lawyer's answer, and I am a lawyer even though I don't work in the FDIC's legal division

anymore. The supervisory guidance does not have the full force and effect of law that a regulation does. On the other hand, I would say to you that supervisory guidance is a very well established technique in the banking industry, and the financial institutions we regulate pay great attention to guidance, and to a certain extent, treat it very similar to being regulations. They understand that when an examiner walks in the door to do the exam, the examiner is going to say to them, I expect you to be in compliance with this guidance, and if you're not, you're going to have to tell me why not and a bank can be written up in the exam for not being in compliance with guidance. Where the difference comes can, of course, is if you want to then go and you want to enforce that legally, there are additional steps you have to jump through, hoops you have to jump through, to effect the guidance which you don't have to do if it's regulation, so that's the first answer. The second question was do we go out for --?

>>Yael WEINMAN

Who do you consult?

>>JEFFREY KOPCHIK

It varies. In the old days, and I have been at the FDIC for 20 years, which I care not to admit but that's what's happened, in the old days guidance tended to just be issued. Banking agencies sent it out. I think there has been a

change in the last 5 years or so where the guidance that I talked about here actually was sent out for public comment because we basically came to the conclusion that we wanted to get some input from the industry, we wanted to get technical and factual information from the industry, as how best to do this, so the landscape has changed a little bit. We're not obligated to send these things out for public comment but I would say that not in every case, but in more and more cases, we're doing that prior to issuing the guidance, giving the industry a chance to comment on it. What was number three?

>>Yael WEINMAN

The third question was, was industry involved and you already answered that one with the second question.

>>JEFFREY KOPCHIK

Okay. They were.

>>Yael WEINMAN

The final question was, is industry clamoring for changes in any areas?

>>JEFFREY KOPCHIK

I don't think the industry ever clamors for changes in guidance and regulation. But I will say that one thing that the staff, of all the banking agencies does, is that we sit back and we look at the guidance and we try to assess whether or not it needs to be updated. Probably the best

example of that is the authentication guidance that was issued in 2005 that became effective at the beginning of 2007. Speaking just for the staff of the FDIC and obviously not for the chairman or our board of directors, the staff at the FDIC is starting to think about and look at the possibility of whether additional guidance should be issued along the lines of the banks took certain steps in 2005 to comply with that guidance, and they implemented certain techniques to better authenticate customers. Have some of those techniques now been compromised to the point where they are no longer acceptable and should banking agencies, for example, in some way point out what those techniques are and basically send a message to the industry that you now need to ratchet it up one more level.

>>Yael WEINMAN

Okay. You did so well on those four, I'll ask one more follow-up which is --.

>>JEFFREY KOPCHIK

Am I being punished?

>>Yael WEINMAN

That's the way it goes. (laughter) Here the FTC, we hear a lot from consumer advocates. I wonder if the FDIC hears from consumer advocates in regards to personal information collected by financial institutions.

>>JEFFREY KOPCHIK

Yes, we do. I mean, I would say that for every time we ask for a comment on a reg or a piece of guidance, we not only get comments from the industry, although most of the comments come from the industry, but these days in particular we will always get at least a couple of comments from different consumer organizations, and from consumers. So they can submit formal written comments in response to a proposal that the agencies put out. We have, you know, we have a whole office that also deals with consumer groups that come in and talk to us. We also meet with them. Sometimes we'll meet with the industry to talk to them. If we do that we always make it a point to meet with consumer groups on the same topic.

>>Yael WEINMAN

Okay. You're off the hook for now. Thank you. Peter.

>>PETER MCLAUGHLIN

Thank you very much. Having seen the effect of Jeff's very good presentation I'll try to avoid doing anything that will yield five follow up questions. I've been asked to speak a little bit about how the states are dealing with security legislation, and it occurred to me as I was thinking about my notes that we have a great number of international people in the audience, or at least people who are perhaps less familiar with the myriad and sometimes confusing U.S. approach to legislation, but the irony is that when we in

the United States are looking at the European Union and how the EU data protection directive has been implemented, there are often a series of observations that implementation ranges quite a bit. And, at the same time, here in the United States, we have the wonders of this sort of Federalist system, so that you will have one layer of regulation at the Federal level, and then duplicative, redundant, consistent and inconsistent regulation of precisely the same thing at the state level. At the state level, we currently have, with regard to data security and the protection and integrity of different types of information, laws in probably all of the states that specifically address data security requirements for Social Security Numbers. At the same time, there are presently, I believe, 10 laws that specifically deal with additional information security requirements. The breach notice laws which were discussed in the earlier panel, and as Marty indicated, range between 44 and 45 depending on how you count and, you know, the fact that New York state has one and New York City has their own, what the heck, and then there are labor laws in the state of New York that address these also. It all makes it rather difficult to manage, which means that ironically, we're now looking to the FTC's safeguards rule and the FDIC's rule for implementing Gramm-Leach-Bliley and thinking, gee, that's not so bad.

There are 3 points that I would like to make. First, what we have at the state level is indeed some recognition that there is the beginning of evolving data security standards. Secondly, that I think we're still struggling with balance. The balance between technology specific and technology neutral, and also, as was discussed earlier, the level of what some might say is vagueness, which I'll talk about in a minute, or, on the other side, a level of prescription that almost comes down to the example that Yael gave earlier, about how the banks need to manage physical security. And then the third quick point will be that of engaging the private sector and different stakeholders and benchmarking. So in terms of evolving standards, one of the benefits that Jeff's organization has is they have been at this a lot longer than most others. So when the states have started to implement different data security laws, of the 10 data security laws that are in effect at the moment, eight of them basically say nothing more than, you know, must implement reasonable security. Now so 4 words, Godspeed. I think that's, on one side, that's a lot of the frustration that the private sector has because, if you're being held to a state regulation of reasonable security, and that's all it says, that doesn't help you an awful lot because the perception, rightly or wrongly, is that the standard of reasonable security is always going to be in hindsight,

whether it's your State Attorney General or consumer protection office, who is coming to knock at your door. But as a practical matter, at the Federal and State level, we do have an increasing recognition of what constitutes reasonable security. You see these in the HIPAA security rule. You see this in the FTC's safeguards rule. You see this, again, at the Federal level in the FDIC's guidance. At the Federal level, the National Institute of Standards and Technology, NIST is very good at developing an increasing level of guidance. The challenge is, though, at the states, it's schizophrenic because you have most of them that have nothing more specific than thou shalt implement reasonable data security. On the other hand, you have the Commonwealth of Massachusetts, which is where I am from and I feel somewhat mixed about that at times. This brings me to the second point, which is that of balancing, the general versus the specific. So on the one hand, it's not enough for legislators to say, you know, please implement reasonable data security without pointing to something else. On the other hand, Massachusetts has, over the last year or year and a half, in response to its breach notice law, implemented a series of data security regulations. These data security regulations have been postponed and have been amended, and while I'm sure that they are tired of postponing and amending, I wouldn't rule out further

postponements and amendments. In short, they have taken a very different approach from that of thou shalt implement reasonable security. The Massachusetts regulations, which are part of a fairly broad consumer protection act require at a policy level a very detailed itemized list of requirements in terms of having individuals who are accountable for programs and policies and developing a series of quite specific programs and policies within your organization. Now, all of this has been prefaced with the usual legislative caveat that we all recognize the different industries and different types of organizations will need to implement this in different ways, but some skeptics might say that the level of specificity in terms of the requirements makes all of that risk-adjusted implementation a bit worthless. Particularly because the second stage of the Massachusetts rules comes down on computer security requirements. Again, this has all been developed with the hindsight of data breaches and so forth, but encryption of laptops, encryption of portable devices, encryption of wireless. These things are really quite sensible in many ways, but as I'm sure Joe Alhadeff might be able to comment, if you're encrypting things at rest even within the network, the performance of your network is going to come crashing down. So there needs to be a balance between the fairly high level of implementing reasonable security and a highly

prescriptive set of rules that allows for very little flexibility. I think that moving forward, following the idea of the safeguards rule where you can implement compensating control, I think that's very helpful. Finally, in terms of benchmarking, one of the things that may benefit the development of legislative and regulatory things in the future is benchmarking and trying to learn from the best practices of the regulators. So rather far afield from the U.S. states, but the country of Egypt is currently developing a cyber security law and one of the exercises they are going through is a benchmarking practice of what other countries are doing. Now, how they implement that remains to be seen but it's a good -- it's at least a good step of trying to find that right balance. So with that, I'll pass.

>>Yael WEINMAN

Thanks, Peter. Just one comment to the panelists. The number of follow-up questions is not a reflection on your presentation. No offense to anyone. A couple of questions, though, Peter. (laughing) Am I hearing -- am I hearing that companies are actually looking for more specific guidance from states on what security requirements they need to put into place? That's one question. And second, are you finding that clients are coming to you not only with the question of how do they comply but whether they are required to comply?

Is the law written in such a way that they fall under the requirements in today's world where most companies, most large companies here in the United States, probably operate in all 50 states and beyond. Are you getting questions, do we even need to comply?

>>PETER MCLAUGHLIN

So to answer the second question first, are we even required to comply? I am mindful of my hosts. I do indeed want to get out of here alive. So the hot topic of the FTC's regulations of the Fair Credit Reporting Act come to mind, and that's one area where there has been a healthy debate of whether the scope of the rules as written do indeed apply to me. And again, you know, wanting to sort of be mindful of my hosts I'll sort of leave it at that. One of the challenges is --

>>Yael WEINMAN

Don't be mindful. We want to have a robust discussion so don't hold back.

>>PETER MCLAUGHLIN

We'll talk outside. One of the challenges that companies have is sometimes trying to figure out whether indeed the rules apply to them. Most of the time I think it's a very good faith inquiry. Sometimes it's more of a matter of trying to avoid additional regulation, which is fair enough. With something like the Fair Credit Reporting Act and the Red Flags Rule that have come -- well, for the FTC, are

going to be coming into effect relatively soon, one of the challenges is that in some quarters, there is an implementation perspective, if you breathe, this applies to you. Because if you offer credit, which is, you know, painted other than right now, that defines you as a creditor. I think the regulatory perspective is that the burden is going to be relatively low and I think that you might hear a chorus from the private sector that this is not quite correct. Another aspect is the sort of unintended consequences. So when -- under the Fair Credit Reporting Act the definition of creditor ties back to the -- creditor ties back to the Equal Credit Opportunity Act. It basically means that a retailer like CVS or any number of others that would be captured under the Red Flags Rule as currently interpreted, that could then also pull these people under various state banking laws. You're a retailer, you're not a bank. Oh, but, you know, because of the way that the rules are written, there are just some unintended consequences. These things always happen. One of the important things is to be flexible. So it comes back to your first question of, are companies looking for more specific guidance? Guidance, yes. Regulation, probably not, but maybe. You need to have something more specific than, in the state of California, or Arkansas, or Maryland, or Oregon, or Nevada. You need to have something more precise than you have to implement

reasonable data security because that doesn't tell you how to develop your policy. It doesn't tell you how to develop your I.T. controls to manage all of this data. The flip side is that if you don't structure the regulations in a genuinely flexible enough manner, then you'll end up in a counter productive situation because you'll be trying to apply a one size fits all.

>>Yael WEINMAN

Thank you. We'll move now to Europe and we'll start with Chris. Chris is going to talk to us a little bit about things on the European Union level discussion about member states and one thing that I'm going to ask Chris to touch upon is something we don't hear a lot about, which is beyond the member states, even within a member state, are there different requirements within a particular country. For example, I know Germany has, I think they are called states within Germany. Are there possibly conflicting requirements even within there? Then we're dealing with three different layers. Like Peter said here, Federal, New York State and New York City. Just hearing if there is a comparable in Europe. Chris?

>>CHRISTOPHER KUNER

Thank you very much. My task is to give you an overview of some of the EU legal requirements and a sense of how companies comply with them. Of course, there has been a lot

of discussion this morning about European requirements and I'm sure there will be a lot of further discussion after this panel. And I don't want to repeat what's already been said or what will be said, and I know many of you already know a lot about European requirements anyway. I'll go over maybe at a high level some points and dive a bit deeper into others. The legal basis for data security in the EU has already been discussed and is pretty clear. Article 17 of the EU Data Protection Directive and there are also corresponding provisions of the E-privacy directive of 2002, which is currently being revised. I won't go into that because I know Mr. Klabunde will discuss that in his presentation. The standard in the directives is also fairly high level and vague. It talks about appropriate security measures. These were ultimately derived in the OECD guidelines. There are other, however, I think very interesting and relevant sources of law and practice in Europe regarding data security. Many have the DPAs have -- the Data Protection Authorities, published papers on data security. There is also national laws on data security. There is also various European standardization bodies, for example CEN, is a Brussels-based standardization body, which has published many standards including securities standards. Some of them, I think, are better than others. Many are voluntary but they can be quite helpful. Now, because of EU

law, the directives have to be implemented into national law. We have 27, at least 27 different implementations of the directive and so if you really want to comply with relevant law you have to comply with local law also regarding data security but I won't go so much into local law here. I do have a slight clarification of something that some of my Euro colleagues said this morning involving transfers within Europe. It's certainly true that you cannot restrict transfers from one member state to another member state based on the level of protection. However, there are other potential restrictions on transfers within Europe which may apply -- which have nothing to do with the level of protection. For example, you will always have to comply with the local law where the data is collected, which includes security requirements and if this is not complied with you may not transfer it, even within Europe. There are also layers like labor law which are not affected by the directive. For example, transferring employee data, there are issues and provisions of national labor law which may restrict transfers. And also just cultural issues. There is really sort of a different culture understanding of data security in different member states. For example, I have handled cases where employees in Germany objected to their data being processed in Switzerland, which is, of course, not in the EU, but it's pretty secure country, or in Poland.

Poland is in the EU and they actually have, I think, strong data security requirements than in Germany and the Data Protection Authority in Poland has more enforcement powers than in Germany. So we see sort of different culture understandings among citizens of security. And this also plays a role, I think, if a company wants to transfer data. With regard to restrictions within a country, I don't think that that plays such a big role. It's true in Germany, you do have 16 different states, Federal states. They each have their own Data Protection Authority. It takes different positions on different issues. There is a body that attempts then to reconcile these issues. I haven't heard of many problems regarding security where, say, a transfer couldn't be made from one part of Germany to another part of Germany. Maybe Mrs. Bock when she speaks can speak to this also. But, you know, there are some other Federal countries within the EU, but I don't think this is such a big problem per se. I think it's more just an issue sometimes of transferring data from one enterprise to another and the restrictions on that apply whether it's in the same country or another country, et cetera. Now, there are many other sources of data security requirements beyond the two directives. I would like to point out a report done by a working group of the European Network and Information Security Agency in 2006. This is called ENISA. I was a member of this working group

and we set out to survey different EU regulatory instruments that had some provisions dealing with data security. This report is available on the ENISA website. You can find it very easily if you just put in ENISA into a search engine. We looked not only at data protection areas but we looked in other areas such as network and information security, corporate governance, authentication, intellectual property rights, financial services, et cetera. What we found, this is even limited to legally binding instruments so we didn't even cover things like recommendations or best practices. What we found is, there are very many instruments at EU level dealing with data security. This report is 37 pages long. As I said it's not by any means exhaustive. There tends to be sort of a lack of coordination between them. So many times, you will find different instruments that seem to cover the same processing and you're not sure which one takes precedence. Many of these instruments are directives so they have to be implemented, which means you'll have different national rules as to how they are to be applied. So there is a lot of law and I can't go into all of it here at the EU level, but I think it's important to point out that this goes beyond just the two data protection directives. Maybe to draw some fairly broad conclusions here, I think that the two directives, the general data protection directive and the E-privacy directive were trail

blazing instruments that did adopt a security standard fairly early on in the game with the general directive 1995 and again going back to the OECD principles. There is definitely sort of a lack of coordination among certain security standards in Europe. Many member states still see this as a matter almost of national security and they are very loathed to seek jurisdiction on securities standards of a pan European body. There is more pressure in this regard. There has been reference this morning to, for example, implementations in national law, Poland, Spain, Italy, Finland, et cetera, having very specific security requirements. There are also major political issues in Europe with just getting member states to cooperate and we look, for example, at ENISA itself, which has been sort of under attack and was even going to be disbanded at one point. Now it's gained another leash on life temporarily and was put out in the Isle of Crete, which is not exactly the center of the data security world. One reason might have been to limit its ability to really come up with security, Europe-wide security standards. I also have to say, you know, if you look at all the law in Europe on security you might think, oh, they must have really great security in Europe. It must be much better than in the United States. Well, that's absolutely not true. Over the last year or two, when we've seen more attention being posted on security

breaches we've seen an appalling string, almost never ending, just pointing out two countries, Germany and the UK, where there are almost incredible, unbelievable breaches sometimes involving the same company over and over, over years and years of just breach, letting data totally flow out of the company. So, you know, there doesn't seem to be much of a correlation between having a lot of law and having good security. I think what we miss is good coordination among the different laws. How does business cope? We had some discussion of this in the morning. Different approaches. I think, as Joe said, in many cases, a lot of this is just good business practice. Maybe 80% of it are things you would do anyway and you have to deal with the rest of the requirements on top of that. There are many other things I could say, but I'm sure I'm a little -- waiting with trepidation on the questions now from our chairwoman that she'll have for me. I'm happy to answer any questions later on. Thank you.

>>Yael WEINMAN

Okay. Thanks, Chris. Actually, just one follow up question. We hear a lot about how there is an overall data protection law in Europe whereas there isn't one in the United States. I wonder if within Europe are there different requirements for specific kinds of information? For example, health or financial data? Is there anything additional that companies

need to comply with for the type of data that I've just mentioned?

>>CHRISTOPHER KUNER

Yes. There certainly are some additional requirements in different sectors. You mentioned two of them; financial services and health data. For example, I know in France, there have been specific requirements issued by the CNIL. Many times these are derived from data protection law. For example, in the health, pharmaceutical research field, ethical requirements, and there is a European directive on clinical trials, and many of these things really go far beyond just data protection laws. Many times there are also national. So, you know, there are some extra requirements in some specific areas, but not in all areas.

>>Yael WEINMAN

Now a question or a prompt for some discussion amongst the panelists. I wonder if Jeff and Chris, if you, when you hear from financial institutions, and now most financial institutions don't operate in only one country, if you're hearing about challenges in complying with U.S. regulations as well as European regulations what kind of feedback are you getting from these multi national financial institutions on complying with various data security requirements, that they have to pay attention to, as a multi national institution?

>>MALE SPEAKER

I'll take a shot at that. I think the answer from my perspective is not so much, and that probably is because the comments that I see are much more specific in terms of the financial institutions that we regulate, commenting very specifically on a regulation or a piece of guidance, and the issue that you raise is not necessarily at the forefront of those comments. I mean, I know enough and I talk to enough bankers to know that that issue exists for certain multi national banks, and that they are concerned about it. But it's not something that comes my way a lot. Quite frankly.

>>YAEL WEINMAN

Okay.

>>MALE SPEAKER

I do hear this from time to time. I'm not a technologist so I don't get into issues about what level of encryption should you apply to this data and how onerous is it, et cetera. But certainly with regard to security requirements in a legal sense, we hear a lot from companies complaining, say, about the breach, or just the huge variety and multiplicity of breach notification statutes in the U.S. and also a lot of fear about what's coming in Europe in this regard because we don't have these requirements really yet in Europe. And we're going to get them in the directive, but of course, this directive also has to be implemented so it's

not just that we'll have one set of Europe-wide standards for breach notification. We'll have at least 27 of them.

Yes, I do hear some comments.

>>Yael WEINMAN

And the real winner of that are the law firm lawyers. I'm delighted we have a question from the audience. Bojana. We have a microphone.

>>AUDIENCE

Of course. My question is a little bit related to what you've just asked. I'm asking Jeff and Christ but please, Sophia particularly. One thing that we didn't have time to discuss this morning but it's exactly to the point, we're seeing increased security legislation and regulation. And in order to protect data and in order to put into place those security measures companies are coming up with new initiatives, email scanning, computer scanning for inappropriate software, audit trails, checking, background checks, and lots of that also may conflict with privacy requirements particularly in Europe. So I would like your perspective a little bit. Chris and Jeffrey, and everybody else as well, please. Do you see that -- don't you think we should do something about it? I certainly see a lot of that where I am at the moment. (overlapping speakers)

>>Yael WEINMAN

Why don't we see if they can answer this question then we

can take another just so we don't forget. Anyone?

>>SOPHIE NERBONNE

Thank you. In fact Bojana that was one of my conclusions. Your answer is that I wanted to conclude my presentation saying that, at the same time, we see that security requirements increasing, as a consequence of the increased privacy related breach. At the same time the monitoring of the computers and so the employees is increasing too. In that way as you are speaking about the problematic aspects of it concerning privacy, it's obviously something we have to take into account, but I must say that (inaudible) in his approach improved, imposed for example to record the logs of all users check the good use of the data, so that it's something logical and it's not to be done in a lawful way, it means that we want companies to establish general policy giving the information to all users of what will be -- how the data will be procured and controlled. That's something quite natural I would say.

>>YAEL WEINMAN

We'll take one more follow up question from the audience and then we'll keep going, being mindful of the time.

>>AUDIENCE

Thanks. This is on the same topic. Last week the CIO of Research in Motion that makes Blackberry announced that they will have continuous monitoring as their I.P. strategy

because you can't prove trade secrets unless you can show the protection. I was wondering what you thought of that because it comes exactly on this point of, on one hand, you want to protect I.P., make sure it's not leaking, but you bump right up against these monitoring requirements in different countries.

>>MALE SPEAKER

I'm not sure what kind of monitoring you mean on your Blackberry, monitoring of your emails, or -- et cetera. You're going to run into big problems in various jurisdictions, and I have to say it's not only Europe. I know from having done research projects in other countries in Asia Pacific or Africa, many times this gets into labor law and people forget that. It goes far beyond data protection law and it's not matter of saying you can't do it but there may be conditions on doing it. You need some sort of employee information consent or works council permission, et cetera. We see more and more of these types of services, email monitoring, et cetera, and, you know, the world is different. The world is not -- I don't believe the world is totally flat yet. I think there are still some bumps along the road and that there are some, you know, differences of requirements and if you're a global company, it's part of doing business. It's not always fun or it doesn't always make a lot of sense but it's out there.

>>Yael WEINMAN

Thank you. Now we'll hear from Sophie.

>>SOPHIE NERBONNE

Thank you. I was told to speak about the way the French Data Protection Authority implements and enforces security requirements. As it was already stated the French law transposing data protection directive deals with security measures on a general point of view. The appropriate measures, technical and organizational have to be taken both by the data controller, but also the data processor. Don't forget, the data processor, for the first time the French have the particular provision under the obligation of security of the data processor. That is to ensure the integrity and confidentiality of the personal data. There is a criminal offense not to do so. So there is penalty sanctions and administrative sanctions with that. So what is the process for the French Commission in the application on a daily basis for such principles? Security requirements? We have to consider three different aspects. The first one would be the ex ante approach, meaning verification done when the processing is registered by the commission. More than 80% of the processing notification is done to the commission and I would say even 90% does specify that security measures have been taken but without describing them. In all cases, I mean when the French law as fixed

necessity of a specific opinion of the CNIL
prior authorization from the CNIL such security measures
will be analyzed by the CNIL to be increase or adapted if
the commission considers they are not sufficient. They don't
reach sufficient level. To give you examples, I should speak
about the activities involving sensitive data like health,
whereas it was said previously, data processors have to be
satisfied by a specific law in this health sector. I wanted
to give you another example dealing with the electronic vote
systems in this specific issue the CNIL has elaborated
recommendations providing guidance on the implementation of
electronic vote system and giving very technical and
practical measures to adopt -- to maintain the integrity and
confidentiality of the vote. This has been done by the CNIL
which was considering on one hand the increase of such
processing of electronic votes of voting professional
elections. On the other hand, the lack of security of those
existing systems. 3 years later, the adoption of this
recommendation what we're seeing is that the companies
involved in such are have considered the
recommendations taken by the CNIL are guarantees for their
systems. So they respect such recommendations. After that
first step, I would say that will come and is coming a time
of auditing the system. That's an interesting way to see how
specific guidance, we go to compulsory ones with the risk of

sanctions to be taken by the commission acting as a judicial court. That's a question we could debate later. I go to the second aspect of enforcement and it is the on site investigation, auditing and monitoring, I must say this aspect of the activity of the French Commission has become much more effective since the new law in 2004. To give you an example, it's still less than our Spanish colleague but more than 400 cases last year to compared to only 50 cases 4 years ago. So you see the proportion of the on-site investigations has drastically increased. So what you have, is useful to know that the specific team at the CNIL in charge of auditing has elaborated, technical audit of security measures, and so that's done for each on site investigation. What we discover is the very basic rules of security are not respected. There is no retention time defined for data shared stocked on the shelves. The log in and passwords are not changed regularly. The working station on the server and the computers are not locked when not used after a while. At least our on-site investigation tries to put and establish a set of security measures. To give you a quick examples, in auditing E-banking activities, the main conclusion, the necessity to increase the level of security by not sending at the same time a password and banking information at the same sheet. That was something quite obvious. Also, to use more specific key words. That

was done and I think that was a good conclusion for those investigations. What's useful to add is that to fulfill such (inaudible) process there is the necessity for all European Data Protection Authorities to cooperate in Europe. That would be interesting for us to think about this cooperation between the peers. For example, if a complaint is received for lack of security in France, and the data controller is established in Poland or Germany, or Greece, we contact our colleague and ask them for their help. Such collaboration should appear of course at the international level. I take the opportunity today, being with the FTC to say that would be wonderful to have this possibility. I know there was a possibility, but things changed. Of course, we would have to consider creating a collaborative way of acting in this area. Since 2004 CNIL has an effective power of sanction both financial sanctions up to 150,000 Euros and administrative sanction, with the withdrawal of the approval of the possibility to block data even as for the erasure of data. What we consider is that the entities which have received until now a report on the lack of security have always taken measures to over ride a function, so we're not yet at -- what we're thinking that the efficiency of the sanction in one way makes that -- it's not necessary to take the sanctions because obviously receiving the demand from the CNIL, the companies have already taken steps to avoid

such sanctions. As I was speaking about my conclusion responding to Bojana that I shall end it there and ask for more questions.

>>Yael WEINMAN

Being mindful of the time, I'm just going to ask one question. It's really more of a statement. So the law that now imposes data security requirements on the data controller and data processor, what was the thinking? It just takes you one step beyond? It's really legislating accountability where here in the United States, we would read that in to any requirement, if the data controller passes the information along to a data processor, that data processor would be required to comply with whatever the data controller had been required to comply with. So what was the thinking behind essentially legislating accountability?

>>SOPHIE NERBONNE

The fact that in the French law, there is a specific requirement for data processor implementing some security measures, is from the European directive. The first step done by the European directives, more steps to be taken to recognize the role of the data processor.

>>FEMALE SPEAKER

You now have two people to go after the event if there is any problem. Be mindful of the time. I'm going to hand it straight over to Yukiko followed by Yoram who will remind us

that the world does not revolve around the United States and Europe and there are countries beyond. So Yukiko, take it away.

>>YUKIKO KO

Thank you. I would like to take you over to not just US and Europe and Antarctica but about other parts of the world today. I couldn't agree more with actually Chris when he mentioned the world is really not flat. Maybe the access to other parts is easier now but I really think that especially on data security, since the culture perception of security may be very different. I really feel in the terrain of data security the world is not flat. For example, I think Jeff and Peter mentioned about the guidelines, the United States guidelines, it could be guidance in the United States, but in Japan guidelines are de facto regulations, so how do you know unless you really don't know the nuance of the rules and it could be industry standards, government endorsements, it's so different depending on which jurisdictional country you're in. Also, different types of agencies are involved. It could be financial services agencies in Japan that have more stringent data security requirements than you have. On the other hand Ministry of Economy, Trade and Industry which is more of an E-commerce ministry. They have their own ways of defining security. So within the domestic level, the country level you have different approaches. Of course,

language as well. So, and then I just wanted to say, from the beginning, and now I would like to talk a bit about Asia and also Latin America. And tell you the kind of general trend. I'm not going to go into details of each country because I don't want to bore you with my speaking. But in Asia, I feel like, and this is my personal observation, there has been more emphasis on technical specifications of data security. I think there is a reason why. Concept of privacy has been a bit more Western concept for many Asians. A foreign concept, a concept that's being practiced in many different parts of the world. U.S. and Europe. But for us it was a bit difficult to define. Data security, people thought, well, information security, we can talk about technical specifications, so let's touch on that. And also, I'm talking about Japan right now but there was also a discussion on Sarbanes-Oxley law and there was some corporate governance type of regulations and combined with that, in Japan, data security was spoken more from really technical information security aspects and how you do better governance of your company rather than privacy perspective. Having said that, though, some of you already know that in Japan you have a law and then each ministry has an implementing guidelines. As to how they interpret the law and how they would be enforcing. These guidelines do not go through a Parliamentary process. However it has some teeth.

The industries have been asking what do it mean by a proper measure. The response by the government has been giving more examples, more examples. That became kind of the de facto standard, which has been kind of a good thing and bad thing as well. The financial services agency has guidelines on core -- the more general guidelines on the Personal Information Protection Act but they also have a separate guidelines which specifies more in details technically and organizationally and physically how you need to protect data so that it will be secure. METI, which is the Minister of Economy Trade and Industry has its own guidelines, it's one guideline but it's probably about 70 pages now. Because they started adding more examples in it which was helpful but not helpful with some companies. They have very detailed examples of technically how should you do it and organizationally how you should structure the data security policy. Moving on to South Korea, Korea Information Security Agency leads this. The name itself is obvious, Korea Information Security Agency, and here you also see an emphasis on information security prospect. The agency has developed information security assessments tools and they have audit tools as well. And I think in Asia as well and this is also my personal observation, if the government says these are the tools that we've developed you better take a really good look at that. In terms of law, as far as I'm

concerned, they have -- it's a very long name -- Act on Promotion Information and Communication Network Using Information Protection, and they prohibit unlawful access and system interference which is a little bit more at the high level. So that's, I guess, the part that they cover but I think KISA deals with more of the technical aspect of data security in Korea. Moving on to China, China, I think, they recently just made amendments to the criminal code and made unlawful sales and disclosure of personal data as a crime. There are no regulations per se in terms of data security specific. However, I know there are some standards that they would like to develop. I think Asian governments like developing standards. And I recall that, I think there was a EU China information society project, that's working with the Chinese government to develop data security standards. So I guess that's one thing that's in that country. Maybe just quickly touch on India. I know there is an I.T. act but also coming from the credit reporting agency, we also have a separate law just for us. It's called Credit Information Company law, and that also deals with some data security measures. So, moving on to the other side of Pacific, Latin America, here, I think there is a very variant trends. Some countries have more influence from the EU and some countries are a little bit more trying to take a middle ground. Like Argentina, I remember that on an earlier panel a person from

the Spanish Data Protection Authority mentioned about the security guidelines and there are like three levels and specifically and precisely I think that's what Argentina has. And Chile and Brazil, they have -- Chile has a law, and Brazil has also law as well. As far as I'm concerned, there are no guidelines per se specifically for data security. And then Mexico, some interesting events happening there. Every year they have three bills on data protection. This year is no exception. I think one of the bills that contains, has some data security component to it, which is that the Data Protection Authority that proposed to establish through this bill, would develop and publish data security guidelines. That would have more detailed, I guess, suggestions on what the appropriate measure of data security for companies. That's just kind of a quick overview. Really my point was that it's just so different from, not just region to region but country to country. I think in Mexico, some states have data protection laws that have some data security. I think very high-level laws but data security laws. So there is no one side fits all for a company to deal with this issue, and we have to deal with it, but I think it would be helpful, especially on data security front, since it deals with more technical and sometimes organizational requirements which really requires a lot more efforts on company to change. If there could be more flexibility and keep in good dialogue

with public and private sector, and then really find more practical and realistic solutions. So with that --

>>Yael WEINMAN

What I'm hearing from you, Yukiko, there is common ground on data security and even with that common ground we find ourselves dealing with some conflicting requirements. One follow up question on Japan, you mentioned the different ministries within Japan issue sometimes very lengthy guidelines and I would think that some companies find themselves under the jurisdiction of different ministries. Do they find themselves being faced with perhaps conflicting requirements from the ministries or is there a process within Japan to be sure that the different guidelines from the different ministries are at least, at the very least, consistent and not contradictory?

>>YUKIKO KO

Very good question. Supposedly cabinet office is the coordinating body and The Personal Information Act, it's their law but they don't have the power to enforce it. That is why the enforcement power resides with the ministries and agencies. And they do have a regular meeting to coordinate and, because the guidelines get updated whenever ministries want to update. So you have to have that coordinating meeting. However, I do hear a lot of challenges from companies saying that we follow them both and which one do

have I to go for. For example, financial services agencies guidelines more detail, meticulous and they have two guidelines as I mentioned, which one do you follow? And at the end you have to actually follow both, with METI and FSA. So they typically they seek guidance, actually, they go to the ministry and agencies to seek for the help, okay, this is the situation I have. What should I do? They go individually to those ministries for their guidance, further guidance.

>>Yael WEINMAN

Thank you. Last but not least, Yoram.

>>Yoram HACHOEN

Welcome to the Middle East. (laughing) I want to start with a general comment about data security. There are rare cases where data security should avoid a data breach. Those rare cases are where either the infrastructure is at the state level or really connected to the business model of the company. I'll give you two examples. One is, if you're running a certification authority and you have a data breach that someone has stolen your private key of specification authority, then you're finished with your business. And if you're -- if you have a barometric (ph) database and this database was exposed, then again, you're in deep trouble. But in most cases, with data security, we're talking about measures that have to do with the probability and the damage to

bring us to something which is reasonable. Not to avoid. Even if you apply the proper measures, you can find yourselves with a breach and what we have to do is really to see that we are diminishing, or minimizing the threat but we cannot eliminate it. This is a general comment with regard to data security. I would like to speak a bit about data security standards. And this comes from my position, both as a regulator of data protection, and I'll explain in a minute, and also, I came from the private sector and I was the first man in Israel to apply ISO standard 17799 for the operation of the certification authority that I have managed. So I have both views of applying security measures. The function that I'm now currently establishing as a minister of justice is a unique Data Protection Authority because we're in charge not on let's call it classical data protection, meaning privacy, but also we give licensees to credit information services and to certification authorities that according to Israel electronic signature law so we have a wide view of data security and we also do a deep audit -- we examine the organization that get licenses from us. There are two types of security standards. One of them, I would call it technical family of security standards, meaning standards like the fips or the (inaudible) which they give an accreditation to a specific device. And you can see, we have it in the Israeli legislation that for certain

activities you need specific accreditation for specific device, I believe that in the future we will see that if you're talking about encryption, for instance, then we may see a requirement for specific fips/(inaudible) approved device to be used. Instead of saying something like general to have something like to have proper encryption means. My experience with those kind of standards is, they give you a high certainty as to the device. If it's past the accreditation of fips or common criteria then probably the device is good. And you can use it. But the problem with such -- with such standards is, that sometimes it triggers the evaluation of the technology because fips approvals, those common (inaudible) devices, their approval is for a particular firmware or software version and if you have a device which is a bit different, maybe it's better but it's not passed all of those procedures of accreditation, then you're stuck with something which is written but it has to be fips approved level, something like this, and you cannot move to better devices. So this is something that we have to keep in mind. And the certification process is very, very rigid. So these are the pros and cons of this kind of standards. Now, the other family of standards is what I call management stuff. Standards like ISO currently 27001 which is in Israel, by the way, we have it as a prerequisite for to get a license to act as a certification authority or as a

credit information service. So if you want to apply to get a license in Israel for this kind of activity you need to present that you have an ISO 27001. If you -- the advantage of such standards, is that they are very wide open and it's kind of a checklist. If you take this checklist seriously and you really pass through the 27001 list and check your organization, and you follow the general instruction of the standards, then you will find yourself with a quite good security policy in your organization, because this checklist is quite wide and it looks at most aspects of data protection, of data security, or information security that you should take a look at. But my experience with ISO is that unless you really came with open heart to accept those kind of standards and you built it into your culture, the culture of your organization, then you can see accredited 27001 companies that do not have information security culture, and on the other hand you can see companies that do not have accreditation but they have very good information security culture. On the general level, I believe it will assist to you build an organization with an information security culture. So I just have 1 minute left. I'll pass it to Yael. And then because we're running out of time.

>>Yael WEINMAN

A couple of follow-up questions. Who can certify in Israel that a company is ISO compliant?

>>YORAM HACHOEN

In Israel it is the Israel National Standard Organization, which are acting under a license of general -- it's not international because it's not something that is being licensed by ISO. The mechanism is not that clear. I don't know exactly how it works. Who really is being approved to get certification. But we've checked it and Israeli National Standard Institution is able to give to those. It's not an Israeli standard, by the way.

>>Yael WEINMAN

Uh-huh. Can you just clarify, when you were talking about devices and certain data requirements of devices, are these devices that can then be sold on the market to consumers or -- so any device be on the market to consumers has to comply with -- .

>>YORAM HACHOEN

No, not every device. The devices that I spoke about for instance for electronic signature, the device, if it's a smart card then it should comply with fips something approval. If we're talking about regulations like I want to see, let's say someone, a hospital, which has a lot of very sensitive information, uses a specific device, encryption device, that is used to encrypt this information, then this device can be fips or (inaudible) approved as a mandatory requirement by the regulator.

>>Yael WEINMAN

Okay. Thank you. Mindful of the time, I think we just have time for a couple of questions. Jetty.

>>AUDIENCE

Thank you. I'm Jetty Tielemans from Covington in Brussels. I have one observation more than a question, maybe to a question. It's actually something you said, Yael, and it has to do with the fact that, in the European 1995 directive there is a specific security obligation on the processor. You asked Sophie why that is. I was not present at the table when the directive was being written and prepared. But it's actually, when you think about it it's actually quite remarkable because the entire directive is sort of geared at the controller. The controller is in charge of all the data and all the other players around. The only thing they "need" to do is follow the instructions of the controller. So it's a very specific exception for security -- for the processor, which I think is important to mention. What is also, I've seen it in my own practice, it leads to some very interesting intellectual and not intellectual debates. Because of differences in the levels of security and sophistication in the security measures within the European countries, you can imagine a situation where these things happen, where you have a controller in a country with a very robust security practice and policy, Spain for instance, and

you would have a processor in a country with (inaudible) in the middle, which country that might be. But those things exist. You have your processor sitting there, obviously, being fully familiar with his own requirements. And you have legal obligation to fulfill those requirements and you have your controller, sitting in Spain and says but what you're doing is not enough. Because I'm under my own legislation and I need to make sure you do X and Y and Z and you have your processor saying I only have to do X under my own country. It leads to very interesting debates. Hot debates, I would say. And it's just something that I wanted to share with the audience.

>>Yael WEINMAN

That's very interesting. Any other thoughts from the audience? Okay, I'll make the administrative announcement then or let Trina come up to make the lunch announcement and what's in store for the remainder of the day.

>>FEMALE SPEAKER

Thank you. Thank you Yael and thank you panelists.

(Applause) This morning we spent a lot of time on Marty's idea of compliance, and this afternoon we'll move more into the risk management. We'll start with the panel on the current practices in the industry and then we will move on to the hot topic of breach. So please return from lunch at 1:30 and we'll get started then. Thank you.

