

>>KATRINA BLODGETT

Okay, thank you, everyone. I'm sure that you're sick of seeing me so I'm going to be very brief in introducing our panel. Our final topic today is data breach and this is, of course, a hot topic. For consumers, a breach is really the public face of data security. It's an out-of-sight, out-of-mind thing but when it comes into sight consumers react. Likewise, there has already been some discussion of how reputational risk motivates companies to avoid breaches but when they happen, the results can be devastating. We're going to talk about what follows when breaches do occur. Our panelists are David Medine, a partner with the law firm Wilmer-Hale and he'll start with general guidance on how a company should respond to a breach. He'll be followed by Russ Schrader, associate general counsel of Global Enterprise Risk and Chief Privacy Officer for Visa, Inc. He'll talk about the third party non-consumer caused by breaches which in this case is how Visa as a brand is harmed by breaches by third party merchants and the incentives this provides to Visa to create and enforce data security and breach response standards. Stan Crosley is the Chief Privacy Officer of Eli Lilly and Company. He'll give the perspective of a company that has suffered a breach and emerged with a stronger, more integrated corporate

structure. Achim Klabunde is the team leader in privacy, trust and related issues in policy development for the European Commission. He will present the state of breach notice legislation at the European level. And finally, very far at the end, but certainly not the least, Kirsten Bock, the international coordinator and head of European private certification at EuroPriSe. She will talk about the potential data breach notification law in Germany. David?

>>DAVID MEDINE

Thanks Katrina. And thanks to the FTC for having me back. What we're going to talk about today is despite the best efforts of the prior panels to prevent security breaches sometimes they do happen. As David Hoffman said just a few moments ago, it's impossible to be perfect in the security arena and sometimes people are far less than that. I'm going to talk about some best practices with regard to what a company should do when faced with a security breach and I think these cross-national boundaries because every company with customer data is pretty much in the same situation. The first thing to think about is that every company is vulnerable to security breach. And so the time to start planning for security breach is not when you've had a breach. The time to start planning is now if you haven't already, and every company should consider having a data breach plan in place, because I can tell you from experience

in dealing with dozens of security breaches, when someone calls you and says someone has just hacked into our computer, that's not the time to figure out your procedures and how you're going to handle the breach. When things are nice and calm and quiet, that's when to do the first couple of things. The first is to put together a written plan to identify employees in the company who will be participants in dealing with the breach. It really should be interdisciplinary within the company. You want to involve the I.T. department of course, but also the business people, legal department, the communications folks, perhaps marketing, because all of those people in the company have a real interest in what happens and how the company handles a breach. If you can handle it successfully it can be either neutral or potentially a slight positive and we certainly know what happens if you don't handle it well. One of the key things after you've put your plan in place, and by the way I should also say one of the things you might consider doing as part of your plan is to draft a sample security breach notice. I can tell you how hectic things are and the time to start getting the buy in from corporate executives and communications and everyone else takes a while. So even though you may need to change it and tailor it to the particular breach situation. Now is the time to do it because different states in the United States require, they

require different language and contents to notification, and again, this is an ideal time to do it, before the breach occurs. The next step is training employees. And this may seem like a simple matter but employees need to be trained to identify when there has been a potential breach. And when they think there might have been a breach to report it up the line as quickly as possible. The next thing you want to have is almost a breach ideally form that guides the process of investigation and also requires people to document what they have done in the course of investigating the breach. Okay. So once all of that has happened, you get the call and the legal department or whatever department that's handling the breach, they say, we may have had a breach, what do you do? You start the investigation. And for those who haven't been part of this process, one might think from the public policy debate, that the easy part of this is figuring out what happened and the hard part is what to do about it. I would say it's exactly the opposite. Finding out what happened is enormously challenging, and usually it's much less challenging to figure out what to do. It's challenging because not every company has a complete audit trail in their computer system that tells you exactly who intruded into the system, when, and what information was copied or destroyed. Oftentimes you have to do it through inference, through circumstance, and there are breaches that I've been

involved in with months and years later you still don't know what happened despite best efforts and intense efforts to figure out what happened. So finding out as much as you can about what information was compromised is enormously challenging. Of course, you have to look at other factors that relate to ultimate legal issues, was the information that was compromised, whether it was on a laptop, a tape or something else, encrypted or not? Many countries and states look -- regulate breaches involving paper records and electronic records differently, so you have to assess what kinds of information was compromised. One of the key early decisions to make is whether to hire an outside forensics firm to conduct the investigation for you. More often than not your I.T. department will say we can handle it just fine, thank you. And also, at least oftentimes, you want to go outside for a number of reasons. One is, your I.T. department is not trained in security breaches, and to identify indications of breaches, to always identify all the potential weaknesses in your system so it's often very helpful to get an expert firm to come in and to analyze that. Second is, an expert, an outside firm, has more credibility if they draw a conclusion as to what happened than the inside people who obviously have some bias because they are the ones that typically design and operated the system as opposed to a neutral third party who does this for

a living and can call it the way it is. And then third, oftentimes you can claim attorney-client privilege depending on how the outside investigation is structured and that, again, for legal reasons may be in the company's interest. An early decision again is to decide whether you can do it yourself or to bring someone else in. At the same time that you're investigating the breach, there are two other things that ought to be going on simultaneously. One is mitigation. Because once there has been vulnerability in your system, you want to make sure you shut it down so you don't cause any further harm. It's bad enough, whatever harm that may have occurred already has occurred. But you certainly want to stop it since you're now on notice there is a problem and that can involve shutting down systems, changing passwords, changing account numbers, whatever it takes to stop the problem will be of critical importance both to protect consumers and potential liability of the company. Then a third thing that should be going on is to start thinking about prevention. Not only do you want to stop the immediate harm but you also want to think about how can we prevent this type of thing from occurring again in the future. That may be because it was an internal person, as we've heard, and one of the things that we've learned in the security area for years now is that internal threats from employees are equal or greater than external threats. So keeping track

of employees nowadays using thumb drives or memory sticks, you can download the whole company's database and walk out with it without you even knowing about it so there are some huge challenges there. Once you conduct and finish the investigation, then it comes time for an assessment of what you have learned. You've got to determine what kinds of data was compromised, where the people live whose data was compromised. There are over 40 U.S. states that have data breach laws. We're seeing Europe actively considering data breach laws and we have to determine whose laws might be implicated by the breach. Many laws have a risk analysis, whether you need to give notice ultimately to the affected consumers, it depends on the potential risk of the compromise of the data and there are new laws coming out on the books. Just recently, in the last couple of weeks, there are health privacy breach notification requirements, and so it's something you have to keep on top of because the laws are changing all the time. There are also timing issues with regard to notifying. Sometimes you have to notify the government first, sometimes consumers first so you have to take care of that. And almost all the laws say to do it in the most expeditious manner possible, puts a real imperative on conducting a prompt investigation and then coming quickly to an internal decision, which again seems simple but it's not. Sometimes people in the corporate structure don't want

to take ownership of the decision but you ultimately should designate ideally a decision maker who will make the tough decision on whether to provide consumer notice or not. Once you've done that, you've got a communication strategy. Do you tell the world what's going on? The question all along is do you involve law enforcement? Some breaches clearly involve potentially criminal activity and sometimes law enforcement will ask you to not communicate publicly about the breach while they conduct an investigation. Many breaches don't involve criminal activity and you don't necessarily need to involve law enforcement. That's a decision that needs to be made. But then do you disclose the breach, give notice where you have to give notice or do you give notice across the board because you think it will ultimately be helpful to consumers? I guess the last thing I want to mention is having been through the process, I think, this panel may be a good opportunity, among others to sit back and decide how helpful is notice to consumers at all. I would be curious, people who have received notice, if they have done anything in response to the notice and what the purpose of the notice is. I'm not sure that the law is currently today, are designed to provide notice, where it will actually be helpful to consumers and not provide notice where it will just be troubling. Consumers may have to take a lot of actions they don't need to take in response to the

notice so the question is, can we fine-tune the process of providing notice where it's helpful? And then ultimately, are we providing notice to the right people at all, which is, do we want to provide notice to current customers or do we really want to provide notice to future customers? So because a lot of what we've seen in activities, people cancel their accounts because they no longer trust company. The question is, would companies be more responsive if this were publicly known, say, on the Federal Trade Commission's website or someplace else, where they can shop around and see where their information is best protect their information and is that a more rational way of having decision-making than the people whose data has already been lost closing their accounts maybe when it's too late. With that --

>>KATRINA BLODGETT

Thank you, David.

>>RUSSELL SCHRADER

Thank you very much for inviting me to join and thank you for the FTC for holding this privacy forum. I want to pick up on something that David just mentioned. That's the importance of trust. One of the biggest things is that people, when there is a breach, when they get a breach notification, is they fear they have lost trust. They have a fear of identity theft. They have a fear that their card

will be used in fraud in any commerce situation. They fear some of the data will be stored incorrectly by a merchant without their permission or for unintended uses. That's one of the major things that Visa is concerned with. Maintaining the trust in the Visa system, of the cardholders, merchants, financial issuers of the charge, the acquirers and participants all have trust in the fact that the Visa system is strong, robust and worthy of that trust. We're concerned certainly about the financial losses to issuers, to acquirers and merchants, when fraud occurs but we're also very mindful that consumers are protected under Visa's zero liability which doesn't undercut other concerns of data losses and potential identity theft but they are not liable for unauthorized consumer transactions. We're also concerned about the use of the Visa system generally. People continue to use it and that you don't go back to using checks and cash and things that they have become comfortable with in the Visa system. So what's our role in this and how do we try to continue to keep the trust that we've developed in the Visa system? We have a bunch of different streams that we work with. The first one is to secure the payment environment. And you've read a great deal about our PSIDSS that we introduced in 2001, which is the payment card data security standards. The PSIDSS initials are probably familiar to everyone in the room and the different steps and

standards that we have promulgated both for ourselves but also working with all of the payment card brands, and a separate standard setting organization of the payment card groups putting out constantly evolving standards for people to live up with. The second thing that our role is, is monitoring identifying and preventing fraud. One of the things that Visa has introduced is called advanced authorization, which is a real-time scoring of an authorization going through the Visa system as to what the percentage of probability is that this particular transaction may be fraudulent. And that ties into some of the things we heard about in the last panel. That's something being out of pattern rather than just out of compliance. And if it's something, for example, you've only shopped locally in a certain area and suddenly, 2,000 miles away large purchases of jewelry or electronics come up, that would be flagged as being out of pattern, and a fraud scorer for advanced authorization may be higher and given opportunity to sort of flag that to see whether it's actually a fraudulent transaction and try to secure the environment that way. A third role that Visa plays is managing the impact of fraud. We have developed the CAM system, compromised account management system. When we become aware of a potential fraud, we take the account numbers that have been identified with the potential fraud

and send them to issuers for their information and for their action. They may choose to monitor them, they may choose to set different parameters. If X number of transactions occur in a period of time, a velocity check, ask for information. If X dollar amounts get charged when it's out of pattern, ask for additional information. It may go as far as having to reissue a card when actual fraud has been shown. This allows the issuers to take varying degrees of tools, depending on the degree of potential fraud to be associated with it. A second tool is our account data compromise recovery system. Our ADCAR system, that helps apportion liability and apportion appropriation compensation for the costs associated with a data security breach among the different participants in the Visa system. A fourth role is maintaining trust in the system. We do this through a great deal of education and outreach. We talk to merchants and issuers and acquirers. We're constantly meeting with the secret service and law enforcement people around the world to educate them about the system, to talk about different tools and to talk about developments that we have seen that will help craft, and bring to justice the people who are breaking the laws and going on. But we're trying basically to create an environment of partnership. That all of the stakeholders are constantly working together to strengthen the trust in the Visa system and to tighten security and

payment systems generally. One of the things that you've read about recently is PCI validation versus PCI compliance. And whether in the case of -- somebody can say they have been validated as PCI compliant, and because they have a validation certificate on the wall, and I think the difference is, and we want to be clear about this, is that a PCI validation is a point in time. That it is an audit. The PCI compliance is a lifestyle. You constantly must be vigilant. You constantly must be bringing in new mechanisms and looking at new tools. 24/7. For example, you can have procedures to detect intrusions but you might need to have the staff and you need to have the procedures to look at the logs. You need to look at warnings, address potential threats, and it must be done on an ongoing basis. You can't say that you have received your validation by your quality assurance at a certain date, and then just put it away and wait for the next one. It's an ongoing lifestyle that people need to work with. As our compliance rates rise in PCI validation and compliance, we've seen new threats. The first one is we've gotten excellent PCI validation for merchants. So now the crooks are moving after processors. As merchants and service providers have stopped storing data, the crooks have moved on to sniffing attacks. As PCI compliance goes up in large merchants, we've seen the criminals go after smaller merchants as well. So they are

very nimble and that's why we're ramping up our PCI compliance programs across the board throughout the players in the industry as well as globally. When we've been moving PCI globally, we've now come to a consistent definition of the merchant's levels one through four that we use, the largest, the internet, and very small people. In September, we prohibited data storage for one and two level merchants and next year we're going to be validating PCI compliance for all of our level one merchants globally. We're also aligning service providers with on-site audits and scans and assessments. It will be additional tools that we'll be rolling out including a global application for service payment providers and that will be rolling out in the next year or two. In summary, I guess, it is an act that requires vigilance and partnership. We've been working with the issuers, acquirers, merchants, processors and cardholders, and each of us has a separate role to play.

>>KATRINA BLODGETT

Thank you, Russ. Stan?

>>STAN CROSLEY

Thank you very much. I joined Eli Lilly and Company about 11 years ago with the idea that I would use my law degree and my biology and chemistry degree, and foolishly thought I would be successful, so I am a privacy officer. I'm not really sure how that works. One of the things I've learned

as the assistant general counsel is that medical researchers really hate uncertainty, and lawyers really, really like it. So not only do I have that fight in my company but I also have it internally within myself. What I'm going to talk about here is Lilly's breach and for me that will be a painstakingly long conversation and I'll talk about Eli Lilly and Company's response and hopefully appropriate length around the why. We had the inauspicious pleasure of being the first high-profile breach case in the U.S., which was prosecuted by the FTC, or perhaps one of the first. I think it was pretty much the first.

>>KATRINA BLODGETT

You can claim that title.

>>STAN CROSLEY

I didn't see any objections from my colleagues. In 2001 we sent an email to consumers and we sent about 700 of them and we sent that email with all the email addresses in the "to" line instead of Bcc line. To Maureen's question, I consider this person a happy, absent-minded Purdue grad. Since I went to Indiana University. I lay everything I possibly can at Purdue's feet. Even though this person graduated with honors from there, it wasn't enough to avoid this breach, and really that kind of underscores the issue here that we're talking about, is that we had a privacy program at Eli Lilly and Company at the time. We really initiated the

privacy program in 1998 and talked about it. The problem was that we didn't integrate with it our security program. We didn't have an easy way for our Purdue grad computer scientist to actually comply with using the security provisions. In the failure of that link, it led us to quite a bit of pain as a company. We know that she understood about privacy, because within seconds of sending the email out, and she actually constructed, in her code language, she put the parentheses, one line, too late. So that the nested loop populated and then sent instead of populate send, populate send, populate send, something like that anyway, and we knew that because a moment after she sent the email, she called me. And she said, I have just made a terrible mistake. We used that as part of our argument to the FTC that we actually had a privacy program, which got us through about the first five minutes of our conversation with them, and from then on, it was a very painful conversation about the lack of security. I will probably always deny that Eli Lilly and Company deserved a consent decree from that activity. Let me be very clear, the FTC was absolutely right as far as how seriously we were taking this issue. And because of that, because of that commitment that we believed very deeply that our patients, our consumers, expected far more from us, we launched a very extensive privacy program. Ironically, to some extent, the email breach, the breach

that we had, would not have triggered any of the current state or Federal or HIPAA breach of state security laws, notices, or international standards. Also, probably more fundamentally, neither would it have triggered if we disclosed the DNA sequences that we have in our biobanks. So you think about that, you look at the security breach standards and you wonder, okay, exactly how are we going to construct our privacy and our security program? Are we going to construct it to comply with security breach notices, or are we going to construct it to comply with what the patients and consumers expect? We chose the latter and we've launched into an extensive privacy and security program, and trust me, they are well integrated now. The layers of privacy and security include policies and procedures, training, technical security measures, with access and controls, as well as audits. Business unit and global affiliate, self-assessments, vendor contracting and certification. We also, however, and this is referenced on a panel earlier, we removed information that was not necessary for us to have. We went back and we redacted Social Security Numbers from almost everything that existed. And it was in places we had no idea a Social Security number would be. We removed unneeded sensitive data. Consumers would give us the information on our websites. We realized we didn't need some of the information we were collecting and that practice

continues today of making sure that just that which is truly needed is what is being collected. The other thing, though, that we realized is that we're a highly regulated industry. And so the clinical research data, any data that makes up a data package or a marketing program is heavily regulated by the FDA. It's called 21 CFR part 11, that's a very extensive security regulation for our industry. It did everything that we needed it to from a security perspective except restrict access to actually view the information. And so privacy had and data security had a layer on top of this, that allowed us to then comply with multiple regulatory agencies and multiple geographies. It's interesting as we went down this path, one of the things we realized that our vendor relationship was perhaps the most critical thing we could have. We took care of things in-house and quickly turned to vendors and put into place a self-certification process, with the vendors and then backed that up with a very extensive vendor privacy standard. Then we have a global challenge, which was a lack of harmonization across the global geographies that we work in. Not only is it a regulated entity but it's a multi-national industry as well. So we've had to use an analogy of a plane, and so we've had many of our geographies who have asserted, we don't need to comply with the privacy standard and the data security standards in Spain or Germany. And our response is, we can't

fly the plane that low. We can't take a plane and fly it at 300 feet above sea level and then alter the altitude every time we come into contact with an obstruction. We have to fly at 40,000 feet, pressurize the cabin, train on emergency services and hope we don't have too strong of a headwind, and that way we can comply much more efficiently, cost effectively and safely with the security standards that we're facing in many geographies. Sometimes the headwind can be extensive. That's where we come back to the goal. Our goal, when we look at where personalized medicine has come, from a circumstance where diabetes was a death sentence 80 years ago and now we have intricate sensitivities where we can mimic certain aspects of the endocrine system, and that personalization required an enormous amount of personal information and clinical research. The same thing about oncology. Cytotoxic treatments are very targeted. You have things like Herceptin (ph) which uses a protein synthesis targeting to do gene testing to determine whether or not this drug will actually work on you. If you over express her two then you have a 50% better likelihood of the drug actually working. So that personalization that is critically important. And what we've determined is that we want to try and be sensitive to what our patients and our customers desire and need. And work the regulatory agencies to craft the regulations that allow us to do that. But before we can

get into conversations around whether we should have genetic material or how we should handle it or when we should notify individuals that they may, in fact -- we may have a drug for their lymphoma, the prerequisite is security. If we don't meet the data security requirements, we'll never be able to have the privacy conversation. I think that's how we've tied it together at Eli Lilly and Company.

>>KATRINA BLODGETT

Thank you Stan.

>>ACHIM KLABUNDE

Thank you, Katrina. Just one personal remark. Sitting next to Stan takes me back to the very beginning of my career when I was working with a company that produced I.T. systems, which were used to record data of clinical trials and one of our sales pitch was the case of Eli Lilly and Company at the time, when they were able to prove that thanks to their documentation system, that they had done everything correctly in the case, and were acquitted of the charges having broken. It's quite interesting, like 30 years later to see them again at the forefront of solving general issues. Well, to come to the topic that I'm going to talk about, I said it already this morning. Whatever I say is my own view and does not necessarily reflect the opinion of the European Commission. But I'm going to talk about the proposal that's on the way in the European parliament and

the council, which is the council of the 27 governments that make up the EU, to introduce breach notifications, mandatory breach notification in the law, and the directive on privacy and the electronic communications sector. The commission made its proposals back in 2007, and since then, institutions have been debating the issue, and those have in the meantime issued the first position on this. Different from what the Commission proposed and different from each other as well, much of space (indiscernible). Though all parties involved have at one time expressed a view that they would love to have result and a agreement before the elections of the European parliament which will take place in early June, so that we get the project through in this legislature, it's, of course, depending on how things the negotiations proceed and no one can confirm that's going to happen or what will be the situation, whether will have to continue with the new parliament. It's certainly not impossible that that's going to happen. Why did we make this proposal in the first place? And why did we make a proposal for the telecom sector? The first answer is it's a bureaucratic answer. It's just that this directive was up for review due to the agreement that the legislators had when it was reviewed the last time, which was in 2002, and there was a clause incorporated in the directive, say, 3 years, after the member states had implemented -- make new

proposals to go forward. This is part of the general view of a larger package of electronics communications related to EU legislation and their directive is one. And the whole package had a stronger focus on security, not on interrelated to privacy, but also with the inherent security of the communication networks and services and such. It was not only on privacy breaches. That is one aspect that we are going to talk about, but in other directives we have other issues that have to do with business continuity with the security of the service, making sure that the networks are available even in cases of force majeure of catastrophes and this kind of event, taking account of the importance of electronic communications sector for the economy and society as a whole. So this already might indicate that we had a bit more focus on security, and the whole exercise in the privacy part, than we have normally. Okay. Why would we -- that was the environment surrounding. But there is also an inherent argumentation to say that it was wise to look at the electronic communications sector in particular, because it's turned out that the data that we're dealing with, indeed, has a certain specific level of sensitivity, which is not just personal data. That was illustrated by a number of case that we've learned about in Europe in particular, in the telecom sector in Germany. Interestingly, these cases happened over a period of 4 years. Some happened last year,

some happened a long time ago, but they only became apparent due to journalists and newspaper investigations which found out things that had been at large for several years, or misused intentionally for several years, without anybody being aware of it. Cases involved malicious employees who stole customer data, often including financial information and sold it. One guy sold data for \$850 Euros and was later fined \$900 Euros, but because it was found that he had played a minor role in the exercise, I understood. One case had a high level of criminal intent when actually, on -- well, probably the highest level management members of communications data, so the data about the communications of trade union representatives, of journalists, members of supervisory board of the company, and even some board members was systematically analyzed to find out who was talking to whom and when and what happened. Trade union members were quite surprised, as they now understood why the employer always knew where the next strike was going to happen. So just by looking at the pattern they would see they were calling guys in a certain region. They could figure out that's (inaudible). This case is very special because it was really criminal intent on the board. It may remind some people of a story that happened in the U.S., in a big I.T. company a few years back. It seems to have some similarity. What we proposed to come back is, we have in our

directive, which is the E-privacy directive, directive on privacy and electronic communications, which builds on the general data protection directive, but particularizes and complements it, gives specific interpretation for the sector of the general directive and adds elements which protect telecommunications data beyond personal data, also legal entities communications data is protected. So it's more business or big business, of course, don't want the data about whom they -- who has been called and so on, to be misused, so this is also protected under the data protection directive. It deals with individuals' personal data and while companies don't have personal data in that sense obviously -- but when they are subscribers to an electronic communication service and they are protected as well. In this directive, we have the security provisions as we have them, we mirror the security provisions as we have some in the general directive. It is, as I mentioned this morning, we have the risk management, measures technical and organizational measures appropriate to the risk. Taking account of the cost of the measure and the state-of-the-art, to achieve the level of protection. The second element, which is also in the existing legislation, which is not mirrored from the data protection directive -- here's obligation of service providers, to warn their customers about risks that the provider cannot do anything about, but

to tell consumers what they can do to mitigate. It would translate, for example, in warning a customer that they should install up-to-date antivirus PCs when they go on the internet or things like that could be used as an interpretation of this. Breach notification scheme that we have proposed builds on these two things. And basically says, when you have done your security measures and you have warned and it all hasn't worked, it has gone wrong, then please tell the consumer as well that this has happened, and so they are in a much bigger risk than they were before the breach happened so they should really now start doing things, if they haven't done anything until now. That's the proposals, and the discussion in both branches of the legislature have basically acknowledged that the concept as such is favored, to be supported, and the discussion has very much been about specifics of the implementation. The question was, should there be a specific threshold and what should be the threshold to trigger notification? Do we have to do it on each and every case? Or are there minor cases where notification could do more harm than the breach? What's the difference between should the regulator, meaning the data protection authority or the regulator be notified every time, and the consumer maybe less often or the other way around? Or what should be the threshold for each and every case? And the procedural aspect were also discussed

controversially. One element where there was a big difference between the two branches was the scope, whether this should cover the electronic communications sector as the commission had proposed and as the council supports or it should also cover anybody who is offering any service on the web, and at that point, there is -- both institutions have taken different ways in their positions on that, and that's a discussion, an issue, of course, in the legislature, ongoing. I see the stop sign is going to rise in about two or three seconds so I'll stop here and I'll be happy to give more details later. Thank you.

>>KATRINA BLODGETT

I'm glad to see you're a law-abiding citizen Achim. We'll go on to Kirsten.

>>KIRSTEN BOCK

Thank you Katrina. Thank you also for the possibility to introduce breach notification draft from Germany and to share some personal thoughts about the draft. Achim has already given you some insight into the situation that we faced in Germany which triggered the pressure for the German Federal government to take some actions and to proceed to amend the German Federal Data Protection Act, which was due for quite a while. So among other issues in January, 2009, they passed a draft bill to amend the Federal Data Protection Act providing also for a provision for

notification of personal data breaches. And the Act aims, of course, to prevent breaches, first of all, but also, to enable consumers to be aware of the risk caused by the breach, and to take measures possible. They need to be suggested by the company that is responsible. To take measures to mitigate the risk. Interestingly, the draft is not limited to security breaches or to sector specific breaches. It covers personal data that are being unlawfully transferred to third parties, or by other means unlawfully acquired by third parties. And it is interesting to notice here that the German wording actually implies that the third party must gain some kind of knowledge of the data being unlawfully disclosed to them. However there, will be some specific sector regulations in the area of telecommunication and media sector, this is due to quite a peculiar situation that we face in our law, having the Data Protection Act, a general act, and a number of sector specific laws and specific Telecommunications Act. But that will be addressed separately. The current draft provision addresses private bodies. Private bodies who store personal data that were compromised. So there is no distinction made between controllers and processor at that point. However, the reasoning for the draft strongly implies that the controllers are addressed, and the reasoning, will play an important part in later in interpreting the law. However, at

this point, the provision or the draft still is in revision, as I'll tell you more details, and there are a number of shortcomings that hopefully will be addressed later on. So the private body who stores the data, that was compromised, is also responsible for notification. And for assessment of the risks created by the breach. Notification will be, according to the draft, will be mandatory only if sensitive data, such as the special category under Article 8 of the European directive 9546 are named. Or if it concerns data subject to special professional secrecy, like doctors or lawyers, also it will be mandatory if data is breached concerning criminal administrative offenses and it was made a provision, especially for data concerning bank accounts and credit card information, as you will be aware, in Europe, these financial information are not concerned sensitive, as listed in the European directive. Special provision has been made here. The notification of a breach of such kind of data will only be mandatory if serious infringement for the privacy rights or the legitimate interest of the subject is dependent. We have this draft addressing each and every breach but only those causing serious infringements, while, of course, the issue is what are serious infringements. And this, according to the reasoning, depends, first of all, on the kind of data that is afflicted, and on the consequences for the data subject

that can arise from the breach. And this includes financial damages as well as social disadvantages. As I told you, the responsibility for notification rests on the private body. To inform, to notify, first of all, the individual data subject, and the data protection authority. This is the case in each and every case. The individual data subject may not be addressed individually if this may create a disproportionate effort, and if this is the case, then a company would have to publish a half-sided announcement in two nationwide newspapers in Germany. And the safeguard to ensure that this notification actually takes place is the provision provides for a fine up to \$300,000 Euros unless the -- this is not an absolute threshold, the \$300,000 Euros if the company saves more than \$300 Euros from not notifying, the threshold can be higher. The German Federal data government -- coming up with this provision, had to solve a conflict of constitutional law, which is also written or dealt with in the provision of the law between breach notification and self-incrimination. According to our basic law, no one can be obliged to self-incriminate himself. So the solution that was found by the government is that whenever a breach causes a criminal investigation afterwards, the information provided in the breach notification can only be used for the criminal proceedings if the person afflicted has given his consent to the use of

this data. Well, the status right now in the legislative process is that there is still a discussion going on. The discussion between the government and the Federal council, which is the representation of the Federal states, and interestingly enough, the roles in the discussions are vice versa as opposed to the roles on the European level. In Germany, the council has pleaded for a broader scope of application and argued that it should not be limited to cases of serious infringement but be broadened. The government has refused to change the draft so far and the next reading is scheduled for the 23rd of March so it's very recent and it's very current legislation that's going on here. The responses of the industries towards this is such that, in general, they find it too strict. It would not be beneficial, therefore the data subject, which is very interesting to notice, they ask quite rightly, why does it only address private body and not public bodies? I think that's a fair question. And they are questioning in general whether the regulation would help to prevent privacy infringement and from that point of view, I will take some arguments that I've heard today so I hope this will be very helpful. But they suggest, the industry suggests that government, rather than introduce privacy breach notification, think of incentives for notification rather than making it obligatory. This is also very interesting

because in the US in this respect has been quite a model concerning breach notification. The outlook for the whole process is that we will have elections in the fall of 2009. At this point, all legislation and process will stop and will have to start again after the election. However, it is pretty clear that privacy breach notification will survive the elections and will be taken up, if the process will not be finalized before the election, afterwards. The status in Germany. Thank you.

>>KATRINA BLODGETT

Thank you, very much, Kirsten, and all of our panelists. I will exercise my moderator privilege to ask the first question but then I want to hear what the audience has to say. The question I would like to ask is, one of the issues that was teed up in earlier discussion has been touched on by several of our panelists is what consumers can do to protect themselves in the event of a breach of non-financial information? And if there is little they can do to protect themselves, is there a value to notice in the situation? And one of the things that Kirsten mentioned was social disadvantage. So consumers must be notified if they might suffer social disadvantage. Is there anything a consumer can do to mitigate social disadvantage or does it just add to the embarrassment? I would say that Stan is also a great person to answer this question, because the breach in Eli

Lily and Company was non-financial information. Any and all panelists, please take it away.

>>KIRSTEN BOCK

I'm glad to answer it. In one of the cases in Germany was about the leaking of phone numbers and related information. There was sometimes financial information involved, but in some cases it was addresses including phone numbers. And there was quite a number of people who did not want their phone number to be at large. There were celebrities of certain levels, politicians, third people with some security concerns, and public visibility or personal issues, where they didn't want to have their phone number known to be protected against stalking or other issues. In that case, obviously, the provider, after they had to admit this had happened and identified the person, one thing they offered to change everybody's phone number without any cost to the people concerned. So it's non-financial information, a very simple case, but that was a measure that quite a number of people concerned, who had this type of concern, also took. So it's a very simple issue actually. Also requiring some action in some cases.

>>KATRINA BLODGETT

Stan?

>>STAN CROSLEY

People should only disclose information to companies who

have a consent decree because we take it so seriously now. I'm not sure there is an answer, other than there is the analysis that everybody does when they submit personal information in exchange for something they perceive that's of value. That's a constant calculation for the sophisticated consumer and it's not a consideration for the unsophisticated consumer. That's why again, especially in the industry that I'm in that you take beyond and you assume what it is that the consumer, what value they put on the information that you have and often you have to look beyond the breach laws to make a determination and put the right program in place.

>>KATRINA BLODGETT

Other panelists that wish to comment?

>>MALE SPEAKER

It's very difficult, once information is out there especially in web 2.0 land, to control and restrict dissemination of information, consumers are actually somewhat luckier in the financial arena because at least in the United States, for instance, consumers who have been victims of breach can put a fraud alert on their credit report to make it more difficult for an identity thief to get credit or even freeze their file to prevent access to their credit information unless they grant specific consent in. In some ways the financial victims are better off.

>>KATRINA BLODGETT

I see that my colleague Al has a question. If you can wait for the microphone.

>>AUDIENCE

This is a question for Kirsten. I was really struck by one of the points you made which was, if notification was too burdensome, the other option is to print something up in the newspaper, I think it was two newspapers of a certain level of circulation. How effective really is that? Are consumers necessarily aware of who actually has their information? I'm certain you weren't suggesting that the names be printed in the newspaper. That would bring up lots of privacy issues, but has there been any research conducted or what's the reaction been to that? And how burdensome is too burdensome, expense or just feasibility?

>>KIRSTEN BOCK

I guess this is one of the issues that still needs some practical trial actually. As far as I know, there has not been any, any statistics on that. The issue was that companies feared they would have to send individual notifications to large numbers of customers or consumers, and sometimes it might even be difficult to address them. Actually, I'm not even sure, you know, if an announcement in two nationwide newspapers will even reach each individual affected. I personally have very, very strong reservations

against this kind of solution. That's the way the draft proposes it, but I think, actually, that a company will be more likely to choose to contact each of its customers on a personal level rather than, you know, going the hard way and making it really public, you know, to each and everyone, in the whole nation. So I assume that this option will not be taken up too much.

>>MALE SPEAKER

If I can jump in there. The substitute notice type of provision that you're discussing is in virtually every state in the United States based on certain thresholds. And it has some very important goals. The first one is that depending on the size of a particular breach, you could bankrupt a small company, subject to breach just in mailing and printing. The second purpose behind substitute notice is that a lot of times you don't have particular personal contact information for the people who have been breached, and rather than ask for it or try to hunt it down, as has happened in some cases, you reach the substitute notice through the papers. The other part is you don't just look at what happens in the two half-page ads in a German newspaper the next day. It's picked up elsewhere. It's picked up in the evening news, it picks gets up in blogs, chat rooms, so from a viral standpoint, virtual substitute notice reaches almost anyone who might be affected in a very cost effective

and a very targeted way. So I would not suggest that you abandon it quite so quickly. When you look at it, it may be a much more effective way of letting people know about problems.

>>AUDIENCE

I was curious, in the two legislative models that are under consideration in Germany and the European Union, how encryption or another technology that safeguards data would come into play. If a laptop, mobile device or back-up tape are lost, for example, let's say there is sensitive data as defined under your proposed legislation, we know it's on there but the encrypted, would that be an event that would trigger notice?

>>KIRSTEN BLOCK

Thank you. Well, we have considered that. I mean, the first thing is what is actually encryption? One expert that I know from one of the universities does a talk every year on the conference, it is the last year in (inaudible). He always has a number of cases where big companies use or recommend cryptography which has been known to be broken for a number of years, at a point in time when it was recommended like an algorithm which had been broken 5 years ago is still in internal developer guidelines of some software companies, so saying data that is encrypted, we don't need to do anything is obviously too short. It has

been suggested in the process of the European legislation to include an exception for encrypted data so the encrypted USB stick or the encrypted laptop does not trigger the full system. One option that is currently under discussion was there should be some judgment by the public authority in charge, that these crypto tools or technical measures, to use a broader term that's been discussed, are, in reality, effective to do the protection. It makes the data unusable. In that case, the mechanism would not be triggered. That's still under negotiation. The proposal has led to the discussion of -- it can only be used for an exception if it's still effective encryption, and the encryption that's effective today will probably no longer be effective 3 years from now. It's a very fast moving process.

>>MALE SPEAKER

Another obvious factor of effective crypto is that the key encryption key be protected. Some US state laws have said that encryption is excluded from breach notification requirements unless the encryption key is compromised which is sort of obvious. In the absence of that, there could be ineffective protection but yet technically meet the safe exception for notification.

>>KATRINA BLODGETT

I'm going to ask another question. This goes to the idea of reputational risk from a data breach and the idea of

deterrence as an effective data security carrot, I suppose in terms of having to give notice. But where the breach is at a processor or other third party, from whom should the notification be addressed? Should it be from the company that the consumers recognize that they have done business with? Or with the company whose security practices caused the breach? I think this is a question that Russ was getting at, in talking about the harm to Visa by third-party merchant actions, so I don't know if you want to start or --

>>RUSS SCHRADER

Well, it's a very difficult question. One that I've given a lot of thought to. And not quite found what to do on it because for example, you take a processor with 250,000 merchants there. And nobody knows who the processor is. And they don't necessarily have the list of 250,000 merchants, and you don't want to get 250,000 breach notices just in case you've done it, so frankly, a lot of it, the first thing you come to, is, in the case of, if that processor, or processing card payments, for example, you would say, you look at it, your statement, regardless of whether the breach has occurred. And so you're looking at it from a cure standpoint and has there been any harm to you straightaway? Does the notice going to do you any good? Perhaps. But only in the sense that it makes you look at your statement again more closely. If the breach occurs at a merchant, you may

recognize the merchant's name and say, oh, I have never shopped there so I don't have to worry about that or I shop there all the time so I better look at my statement more closely, but once again, the action is the same. You look at your statement. You see whether you recognize all the charges that are listed on the statement. If you don't recognize the charge, pick up the phone. Call the merchant if there is a number. Call the issuer, and Visa has the zero liable policy, that it will protect you from any unauthorized charges there. So I think it's less hung up on the fact that this one had to pay for an ad or that one had to pay for an ad or it came through a letter or came from a newspaper ad or it came through a blog or came through an email forwarded to you from a friend, I focus, frankly, more on how do you protect the participants in the system? And that is by doing the kind of standard thing that you should do generally speaking. That is, check your statement. Make sure the charges are yours. And realize that, you have to keep your card safe. Keep your account number safe. But that you have zero liability protection.

>>MALE SPEAKER

I think there is a somewhat broader question because sometimes breaches don't involve, believe it or not, Visa or MasterCard and they involve other companies. So the question then, as a practical matter, how can you give effective

notice to affected consumers? I think part of the problem is, if the letter comes to someone that the consumer has never heard of, if Heartland sends me a letter it will go in the trash whereas if it's a merchant I deal with or a credit card company sends me a letter I'm at least more likely to take a look at it. I was interested in the consideration in Europe having either the controller or processor provide notice because, again, that goes to the question, if the consumer has never heard of the processor, which is likely the case, whether a notice from the processor would be paid attention to, or taken seriously, as getting a letter out of the blue from someone you've never done business with. There was an interesting proposal in Congress about a year or so ago to send all breach notifications in a purple envelope. So that regardless of who it came from you know this is a serious matter. Okay, could you also see the scam artists taking advantage of that as well.

>>KATRINA BLODGETT

Uram (ph) has a question.

>>AUDIENCE

I have a question about the relations between class-action and breach notification. What do you think there should be any possibility to submit class-action according to breach notification; because there is a contradiction you just say to the public, sue me. Okay. So I would like to hear

comments about that.

>>KATRINA BLODGETT

I think as the lawyer in private practice, that's all you David.

>>DAVID MEDINE

It's not surprising that class-actions follow-on frequently from breach notifications. I don't think you have to do much in that regard but getting back to the question of incentives. There is no question that companies these days are very incentive driven, for a number of reasons, to protect information. One is, that any major breach inevitably triggers multiple class-actions like the Heartland case has. So regardless of the merits, it's extremely costly to a company to defend those class-actions and sometimes the merits aren't always in their favor and they pay out substantial sums of money. But I think they are very separate events. The breach notice usually follows at least days before the first class-action is filed, sometimes longer. The other thing I would mention is that at least from what I've seen from clients is that reputation concerns are a great motivator in the space, especially for consumer facing products. Nobody wants to be known as the breach company. They want to be known for the product and service that they provide and we have unfortunately a number of companies who have become more known for their breaches

than for what they sell. It's a very strong incentive for companies to examine their systems. Another incentive that we really haven't talked about is when there is a security breach, it's not only consumer data that's affected, sometimes it's proprietary company data that's affected and that's certainly something that resonates with corporate executives. You trade secrets, your new product line, whatever your magic is for your product, if it becomes known, you could be in serious financial trouble so there are lots of corporate incentives across the board to protect the information.

>>MALE SPEAKER

The class-action piece has had mixed results. What is the actual harm that's associated with it and what are the actual recoveries? For example, you know, I was looking at the Veterans Administration breach of a couple of years ago. Where a laptop went missing with several million names and addresses of veterans. People went crazy. Sending out notices about the breach, notification, and all the rest of it. It turns out the laptop was recovered, absolutely no evidence that there had been any access of it or any misuse of it, and yet, the Veterans Administration has put up a settlement fund of, what, \$20 million for mental distress and actual damages associated with a breach that -- exactly. It's one those things where you have to weigh, you know,

remedy against the actual harm. The other part of class-actions, certainly they are an important part in the U.S. of what happens associated with a breach. But there is also the alternative dispute resolution system that Visa runs, for example, to help mitigate some of the losses that are suffered by parties within the system, and the FTC has a few good friends for 20 years, on relationships, and the state attorneys general is -- has a very strong role as well in enforcing data security, on top of the general reputational risk and harm that's suffered by a breached party.

>>KATRINA BLODGETT

Kirsten, I don't think you mentioned in your presentation, will German citizens have a right of private action or the ability to receive compensation if their information is breached? And to what degree and what was the debate surrounding that?

>>KIRSTEN BOCK

Not according to the bill. They claim they would have to make claims according to the general rule or laws that are provided in this respect. We don't know actually class-actions, as they are common in the U.S., even -- it has been discussed whether a consumer organization should have a right in these notification processes, but it has not shown any effect in the current draft bill.

>>MALE SPEAKER

Another twist in this area is thanks to Visa and other credit card issuers, strong protections both by law and voluntarily from victims of fraud, oftentimes in these cases, the consumer is actually not out any money, and so it's really the banks that have to reissue credit cards that tend to incur the greatest expense in the process. That's where the Visa dispute resolution process comes in, to resolve the payment and compensation to the banks for doing that.

>>KATRINA BLODGETT

Other questions? I'm sorry, yes, over here.

>>AUDIENCE

Leaving the proposed legislation aside, what is the view of the data protection authorities in Germany today as to whether, if there is a breach, individuals should -- or the protection authority itself, should be notified.

>>KIRSTEN BOCK

Well of course we're notified in the number of questions in order to mitigate the consequences. Of course, I mean, we would like to see ourselves in this position, even though this may cause some additional workload on the DPAs. I'm not entitled to speak for each and every DPA, I can only give you some thoughts about what our thinking about this is. We're generally in favor of this kind of legislation because

we believe that the consumer has a right to know about breaches in general. It's about our position at this point.

>>KATRINA BLODGETT

A topic that was touched on very briefly in David's presentation, is the health privacy notice, that was part of the stimulus package, and this is a very new area of law, and it's a new frontier for us and I was wondering if any of our panelists had any thoughts or comments on that, that provision. Perhaps not.

>>MALE SPEAKER

It's similar to the comments that have been made here. It's a delicate balance between, especially with any of the 18 elements that are involved in, that are covered by HIPAA, any of those does it really raise the level of the need to contact the consumer, which could create more stress than actual harm to the individuals and balance with now there has to be robust security programs. Certainly no one wants to have that. One of the primary issues, I think that needs to be weighed in implementing guidelines is the chilling effect that a data security breach notice requirement can have on health information exchange, which is kind of the overriding purpose of the legislation. Certainly is just disclosure of a string of dates could raise the level of a breach notice that will have a chilling effect, especially when outside of the major institutions, only about 8% of

physicians across the country currently have electronic medical records. There won't be a rushing in to electronic medical records environment.

>>KATRINA BLODGETT

More audience questions? Yes?

>>AUDIENCE

I had a quick question, perhaps for both U.S. and perhaps for our European friends. When you have a breach, obviously, there are a number of entities or groups that are adversely affected and we've been focusing largely upon the consumers who are affected, when their information is broadcast out or is compromised. But as David pointed out, there is another class of groups that are affected oftentimes, other people in the business chain who are sort of innocent victims, as it were. Most often, say, a card issuer, which would incur significant expense in reissuing cards or things of that nature. I guess my question would be, for the U.S.

panelists, where do you see that working or not, in how those entities get redressed? I know there have been some issues, movement towards court actions that have met with varying success and Russ has talked about the arbitration clauses for Visa. What's worked in the U.S. and perhaps any lessons learned that they might want to share, and perhaps what the European side is thinking about handling that group of aggrieved parties as well.

>>MALE SPEAKER

I start on that one. I said earlier, our directive covers also subscribers that are legal entities. And so that's basically the subscriber is a party to be notified in any case so the subscriber is a business whose data has been breached, then they would receive notification to do with it what they need to do. The director fully puts the emphasis on the providers of the electronic communication services or networks. We do not distinguish between processor and data controller. It's always the provider who is to detect what has happened and is also responsible for the consequences, even if they have used an outsourcing or processor for the purpose. That's in the proposal so these businesses would be covered but it concerns not only the data that's processed in the name of the provider, not everything that is somehow connected to their service. It is a political issue, which is discussed in Europe.

>>MALE SPEAKER

I think from my perspective, what's worked is that love them or hate them, data security breach notices have put data security in the mainstream, at the forefront of the corporation. I think that's a good thing. However, I offset that with, you know, those breach notices that don't have a harm threshold, I think, can -- you can very quickly move into a numbness with consumers who receive notices that they

don't consider significant or even necessary. And so we have the real potential of just overwhelming consumers with a lot of paper. And the other thing is, if -- if there isn't a harm threshold you also have the potential of moving corporate resources to avoid a risk which isn't one of the risks that we need to be avoiding potentially.

>>MALE SPEAKER

In terms of the economic harm, it's largely been allocated by contract between the various parties, issuing banks, acquiring banks, processors, retailers, although it's certainly the case that probably five or 10 years ago, no one thought about this issue. As a result, contract with the retailers really didn't impose much, if any, liability for retailer for a breach that occurred at the retailer level and there has been a fair amount of litigation that basically supports that position. At least one state, Minnesota has passed a law to try to impose some responsibility on retailers, but my guess is over time contractual relationships will be modified as appropriate to allocate financial risk among the various parties.

>>KATRINA BLODGETT

We have another question up here.

>>AUDIENCE

This is for the lawyers about the linkages between the breach, litigation hold and your records and information

management policies. Does the breach, because there is a reasonable anticipation of litigation automatically trigger a hold and then are you working to make sure you know all the places where you potentially have that information because you have to preserve it?

>>MALE SPEAKER

I think these things tend to happen quickly enough that probably not enough time for your disposal policy to kick in. I think you're going to want to, as I said earlier, document what happened, because I think on balance it will be better to document what happened and be in a position to defend yourself from either an FTC or other government investigation or private litigation. These things happen so fast that I think it would be inadvisable to dispose of documents because oftentimes, these things that happen, sometimes things happen that can't be anticipated. Or you can only screen employees so much and, despite your background checks and everything else, you have an errant employee, who is a criminal, who steals information from you. At least today, for instance, I think the FTC has been willing to recognize that if you have very strong security protections, very good employee monitoring and so forth and something bad happens you may not ultimately be legally responsible for that criminal activity of that employee. And so again, documenting what happened and the procedures you

had in place sometimes can be very beneficial.

>>KATRINA BLODGETT

I'm going to follow on to that question and then we'll take another audience question. I'm interested in the interplay between the possibility or certainty of litigation and the ideal breach response? You had mentioned, David, in your presentation, one of the reasons to hire an outside forensics firm is that you can perhaps claim a attorney-client privilege, not that the FTC is endorsing that position, for the subsequent report, and in that instance, you might perhaps suddenly convey to the forensics firm the required result that they need to reach in their investigation, and you might not investigate deeply into a breach or take all of the corrective actions that might be best, so how does a company balance that tension between having excellent data security and excellent breach response while at the same time listening to their lawyers?

>>MALE SPEAKER

I think it's an interesting observation because in my experience it's quite the opposite, where the outside security firm goes nuts finding every possible vulnerability and is fully free to document it thoroughly in their report. They view that as sort of their job. They don't get paid unless they have found all the possible problems there are and no company is perfect. And so I would say, I can see why

one would think there would be incentives there but in my observation, in every case it's been exactly opposite.

>>MALE SPEAKER

That's exactly right. I agree. The other part is you want to get outside people because you don't know where the breach is. You don't know if internal people are involved as well. You don't know. Part of it, something has happened and you're starting from square one, day one, what happened. And you don't want to say don't trust anybody who works for you, but until you figure out what's going on, you want an outside person doing the look.

>>MALE SPEAKER

I should also add that we're talking about security breaches but to step back to the panel before hand, I think it's also very strongly advisable to hire an outside firm to test your vulnerabilities to see how strong your firewall is, your systems are, see if your wireless network is as secure as you think it is, and to do that on a regular basis annually or bi-annually, just to make sure your security is strong. Don't necessarily rely on your I.T. department who may be very good at setting up the system but look at the people who are experts, ethical hackers, who will try to get into your system and let you know where the vulnerabilities are.

>>KATRINA BLODGETT

Another question?

>>AUDIENCE

It is rather a comment than a question. Following Kirsten's presentation on the future breach notification in Germany, so far, as you know, we don't have a breach notification obligation in Europe. Obviously we're going to have it concerning our telecom industry, but not generally, not for all sectors. So that, so far, whenever there was a breach, which affected globally a company, worldwide, both in the U.S. and Europe, one of the big issues was always, do we need to notify also the breach in Europe? The message doesn't always -- it's not always transferred from the U.S. to Europe. So far, usually the answer was no. We will not notify in Europe [inaudible]. There will be an obligation to notify security breaches in Germany, I think this is going to change completely because, of course, people talk and when there is a global company, you cannot imagine that there should be notification of breaches in Germany and this is not going to be said to anyone in France or UK, et cetera. So, of course, it's going to trigger. Even if I am not going to have an obligation, it's going to change practices very much.

>>KATRINA BLODGETT

So is Germany going to be the California of the east?

>>MALE SPEAKER

Just to react to that, it's not according to our knowledge,

not that we don't have any breach notification whatsoever in all of Europe. It was one of the triggers to come forward with the proposal in the telecoms law that we saw this developing in several countries and we've already rules in place, for example in Finland where there is some breach notification. We hope that we can avoid to have a situation like in the U.S., where we would only have 27 different laws unless we get state laws differing in Germany or some other Federal European states but we're looking at it, of course with the view, and that was what industry required from us when we presented the proposal. Please ensure that we don't have 27 different implementations. Of course, that's what we're looking at.

>>KATRINA BLODGETT

Kirsten, is Germany conscious of its policy leadership role? Did that play any part in developing the legislation or is that an unintended side effect?

>>FEMALE SPEAKER

I think the political situation was such in the past year that they needed to take some action taken. However, I mean, we will have to look at the privacy directive in order to comply to it. Whether there will be any changes that become necessary, you know, because of the directive, we don't know yet. However, they are going to proceed, going to proceed with the law.

>>MALE SPEAKER

This raises questions of extra territorial application of law, because there will certainly be situations in the United States where a U.S. company may have data on German citizens but U.S. law doesn't require notification, and the fact that German law may or EU law may not apply to U.S. companies so there may ultimately be gaps again, suggesting the importance of international cooperation on these issues.

>>AUDIENCE

Hi. I have two related questions. First, picking up on something that was said in an earlier panel that companies have besides compliance and laws. They have independent incentives of reputation to make sure they secure data and respond to a breach. But my understanding, just from my work in this area, is that security is something that's very hard for consumers to know about, and that perhaps the breach notification laws may have increased those incentives tremendously because now consumers know who is the one that lost their data. It's very hard for consumers to know who it was that didn't secure their data. So breach notification laws presumably have increased that incentive remarkably, and the second thing from those of you who are actually, some of you are working with companies, have the data security practices indeed gotten better due to breach notification, or is that something we all talk about, oh,

it's increased the incentives and the data security is much better. Have you noticed that it's better?

>>MALE SPEAKER

I can't imagine anybody who looked at the BJ's warehouse and the TJX breach and didn't say, there but for the grace of God go I. There for the grace of God go my the I.T. guys. There has been tremendous evolving attention paid to data security generally. I don't know whether sending X million notices are the things that drive it or whether it's the bad press or the potential loss or whether it's reputation. But I think it's probably a combination of a great deal of them, and certainly, part of it is standards that are being set for the price to pay to play in the game rather than the breach notifications. The idea that the payments brand have gotten together and proposed PSIDSS and say if you're going to be participating in these schemes you will meet these measures, you will have at the stations of these measures, you will have third party people come in and validate your compliance with these measures, is something that performs probably a greater role and a greater number of participants than just the odd breach that comes up or the fear of becoming the next one. You need to approach it in a proactive way, in a partnership way, and in the positive way to show the importance of data security rather than do it, as I'm afraid I'm going to be breached and have to send out

a lot of pieces of paper. Although breach notification is very useful, where consumers may suffer actual harm, consumers can take some specific tools and steps to protect themselves, in my industry, read your statements look at credit monitoring services, examine your credit report once every year, be very careful and securing your payment card. I would not ascribe the increased level of data security merely to breach notices.

>>MALE SPEAKER

As a chief privacy officer, I would say you heard the four meaningful, robust and predictable regulations that are the ones that will drive practice every time. And that enforcement is, again, meaningful and predictable, and adds some robustness to it that will be far more effective than disharmonized breach state notice requirements.

>>MALE SPEAKER

Of course, there are other laws, and financial institutions that are in the Gram-Leach-Wiley safeguards rules, health institutions are under HIPAA safeguard requirements, the PCI standards are very pervasive because almost every merchant takes credit cards so they are now subject to it. There is no question that the breach notification requirements have been very sobering to companies and I think it would be hard to imagine that isn't true across the board. Companies have better security measures in place today. At least in part

because of that.

>>KATRINA BLODGETT

Joe, I think you had your hand up first in the race.

>>AUDIENCE

Thanks. The question I wanted to raise is a little bit of a follow up to that question, because I think sometimes you might have the wrong incentive that's also created by regulations. So when you looked at 1386, California breach notification law, because it places such emphasis on encryption, there was the run on let's get an encryption solution for everything without necessarily the full thought on the defense and depth strategy. So I think there is a concept that some of the defense and depth concepts are things you want to create an incentive for and it's a concept that was just discussed about the FTC finding, if you have good and robust practices, perhaps the errant employee doesn't create the liability. Just it would be interesting to find out from the panelists how they think is the best way to motivate that kind of broad base defense in depth and not just a point solution because every once in a while something is mentioned in the legislation that gets highlighted and taken out of context.

>>MALE SPEAKER

Thank you for the question, Joe. We have been talking about the broader concept of security in one of the earlier

panels. I think we must also be aware that regulation is not the only instrument and regulation is not necessarily always the silver bullet. Of course, we apply an approach which includes the best practices and exchange of information, and making sure that everybody is aware of the issues and also to do their own interests. But I have to admit information about breaches has been proved to be a very, very extremely effective element in awareness raising whether there is a mandatory breach notification obligation or not, it triggers measures in companies, so it goes together with all the other measures of non-regulatory aspect, which improves the overall situation, and that is the basic objective. It's not to have as much regulation as possible. It's to have a good level and culture of security in the industry.

>>MALE SPEAKER

I would just like to answer that as well. I'm sorry for the sports analogy, but if I was largely playing defense and breached circumstances in trying to convince the company that there was harm that could occur to the company, their reputational aspect, it's a defense-oriented approach, when we started getting traction with our data security and privacy program was when I went back and I looked at what the business was doing, and I laid it in terms of, we cannot achieve the mission of this company and take care of the patients that we want to take care of unless we do these

things. The personal information is too critical to the mission -- the primary mission of the company. We cannot get to personalized medicine unless we can handle personal information. And once we started talking with that, we started talking the language of the researchers and we were saying you will not be able to recruit patients for these trials if we don't do this. And once we turned it, and made it a part of our offensive strategy, then we had a much greater uptake and became a much better private security company because of it.

>>KATRINA BLODGETT

Yes, question.

>>AUDIENCE

Mark McCarthy. What do panelists think of the idea of required notification for law enforcement and for regulators so somebody can keep track of developments in this area and see if there are any patterns of vulnerabilities and defense that might be helpful?

>>MALE SPEAKER

I'm not sure law enforcement so much, first of all, I think it will distract them. In my experience, the vast majority of breaches don't involve criminal activity and so I think requiring law enforcement to assign somebody to take these notices in when there is no evidence of criminal wrongdoing maybe overburdening. The regulator side is a more

interesting one. A professor at Berkeley wrote an article looking at the experience in the environmental area, where firms that have spills are required to notify EPA which then post that information. And apparently that's been a very effective way to incent companies have fewer spills. The argument of the paper is, that lesson would carry over into the data security area.

>>KATRINA BLODGETT

I'm going to ask the panelists one more question, with I hope a brief answer. What is the most important take-away from a data breach or the most important aspect of the data breach response? Is it notification? Is it making consumers whole, which can be accomplished without notice as in Visa zero liability? Is it the ability or the forced time for the company to assess their security program? Is it the integration of privacy and security functions? Let's start with David and go down the line.

>>DAVID MEDINE

Well, the one qualifier, a lot of breaches don't involve harm to consumers. Of those that don't involve harm it's the self-reflection and how to prevent -- let the company reflect on their own procedures and prevent something like that from happening again.

>>MALE SPEAKER

Exactly right. It's the wake-up call. And even if it's

contained, even if it's nothing, it wasn't, you know, an international criminal element that seems to capture everyone's imagination, if it was a thumb drive of a disgruntled employee, whether it was a laptop stolen out of trunk of a car in a parking lot, it was recovered later. Whether it was a FedEx package that fell off the FedEx truck into the snow and wasn't recovered for, you know, until spring, which would have triggered notification laws under a number of state statutes. I think all of those will cause the company to examine their existing processes and to see what they could do better.

>>MALE SPEAKER

We had a choice with could be forever known as the company who had a breach or we could try and put together one of the best privacy programs in the world. And so I think you drive that way.

>>MALE SPEAKER

I would see it very similar to what Stan said. The breach and the breach notification is at the very end of the process. The expected negative outcome for the company should be the measure to bring privacy and security to the attention at the highest level in the company. Before anything happens, serious and effective measures are put into place. We're not going for the breaches, we're going for the prevention and that needs resources and management

attention.

>>KRISTN BOCK

I would agree that the breach notification is at the end of the line, and while we, at least my office, hopes -- or looks at breach notification as a trigger for proactive action, that we like to see, much more broadly, at least, in Europe, and we see also that it actually can have a positive impact also for companies who are offering, at the end of the day, better services to their customers, as we've heard here. And also one approach from my office would be to -- that we would like to see it, a breach notification implemented in technologies and we've done some research in this respect and the prime project that is also disseminated on the website. If you're interested in that, they have made up a case on that, an actual trial and came up with very interesting suggestions in that respect.

>>KATRINA BLODGETT

Thank you very much to our panelists. [Applause] And thank you for attending today and participating in such a lively and interesting manner, and we now invite to you join us for cocktail hour.