TRANSCRIPT

PROOF POSITIVE:
NEW DIRECTION FOR ID AUTHENTICATION

DAY 2 OPENING REMARKS & PANEL 6

APRIL 24, 2007

>>JOEL WINSTON

Good morning, everyone. Thanks for coming back this morning. You hearty souls who arrived at 8:30. And I wanted to talk a little bit about what's happened so far and what's going to happen today. We covered a lot of ground yesterday interspersed with the press conference announcing the release of the President's Identity Theft Task Force Strategic Plan. And for those of you who have had a chance to leaf through the Strategic Plan, you will see a lot in there about authentication and the vital role it plays in the fight against identity theft. So this is really good timing.

Today we have a lot more to cover, but before we begin let me try to summarize what happened yesterday. We started with some opening remarks by Chairman Majoras who, among other things, talked about what we can learn from the Social Security number experience. How the SSN's use as an authenticator has led to increased identity theft. She then challenged us to think about how government, industry and consumers can work together to build better identification and authentication systems.

Simon Davies and Gus Husein started things off with their now famous five D theory even though no one could seem to remember what the five Ds were. I think someone got four of them, which won the award. They discussed, though, a number of challenges in developing an identity policy, from cost, to public trust, to the need for feasible and well communicated goals, to political constraints.

Another key challenge that we discussed yesterday was how an identity system can be structured from the centralized to the distributed, and what the strengths and weaknesses are of each of the different systems. We then heard how current identification initiatives including Real ID, E-passport, improvements in birth and death certificates and the customer identification program, fit into an identity system and what the possible unintended consequences of use of these new credentials are.

We started the afternoon by reviewing the technologies currently available and being utilized in the authentication area. Biometrics, RFID, PKI, Smart Cards, extended verification certificates and risk-based authentication. We talked about the strengths and weaknesses associated with each of these. And in listening to this discussion I was particularly struck by the sheer multitude of possible technologies with new ones being developed all the time.

Then moving from the development of new technologies to implementation, we looked at the challenges associated with employing these new authentication technologies and how different companies and different industries have addressed them.

In the final panel yesterday we discussed the value of multi-factor authentication and the need to educate consumers if we're going to have a successful authentication solution. Unfortunately, there doesn't seem to be a panacea out there. No single authentication system that's going to be simple, effective, affordable and convenient, so it looks like at least for the foreseeable future we're going to have to deal with multiple different kinds of technologies.

This morning I'm going to moderate a panel on the new applications and upcoming challenges in authentication. We're going to look at VoIP, Voice over Internet Protocol, mobile commerce systems and others and their unique challenges and risks. Then we'll end the workshop by taking everything we have learned through the preceding day and a half and try to develop practical ideas for moving us closer to more effective authentication.

Finally, this afternoon we'll have several break-out sessions to explore various authentication issues in more depth. One break-out session will look specifically at the enrollment or identification system and how we can achieve both privacy and security. Another will look at how to bridge the physical digital divide to allow for digital credentials. A third session will explore leadership and collaboration in building better authentication and identification systems. And the last of the sessions will look at the role of incentives and risk allocation in building these systems. We hope that many of you will choose to stay and participate in these additional sessions.

The first day of the workshop I think was a tremendous success and I believe we all learned a great deal. Even those of us as technologically challenged as I am. I again want to thank our panelists and moderators for their invaluable contributions. It is now my pleasure to turn things over to Kristin Cohen who will discuss some of the logistics today before we get started.

>> KRISTIN COHEN

Hi, I'm Kristin Cohen. I'm going to go over a few things. You heard most of this yesterday but it's just a few housekeeping matters and a few announcements.

First of all, the workshop is being webcast and going to be available to view after the workshop in the future. The break-out sessions this afternoon, however, will not be webcast. So again we hope many of you will choose to stay for those sessions. Because of the webcast we ask that the panelists please stay close to the microphones so that we can pick up your voices and speak clearly.

We have a lot of ground to cover today so we also ask that the panelists please adhere to their time limits that they discussed with their moderators for their opening

statements and to be mindful of time when answering questions so everyone can express their views.

I'd also like to call your attention to the four break-out sessions we have this afternoon, they're listed at the back of the agendas you all received. Joel went over them during his recap but I want you all to know these are designed to be a round table discussion so that everyone who attends is able to participate. Although we have set out these topics, they are meant to be a place to start and we've tried to structure them so that the group can move the conversation forward in whatever way they see fit.

Lastly we hope to draft a report based on this workshop so we'd be interested in any comments that any of you have. You can submit your comments via the workshop web page which you can find at www.FTC.gov and you can also mail in comments if you prefer to the address listed on that website. And actually one last thing was that there is material out on the information table outside, including a paper that was written by the first two panelists yesterday, Simon Davies and Gus Husein, as well as the presidential task force report that was issued yesterday.

Then just a couple of housekeeping notes. If you leave the building for lunch, just be aware you're going to have to be screened through security to reenter so please leave enough time to do that. Please wear your name tags at all times. If you notice anything suspicious please report it to the guards in the lobby. Please turn off or set to vibrate your cell phones and please don't use them in this room. It does interfere with our video equipment. Also try not to use them out in the hallway because it was loud and I think some people were having trouble hearing yesterday when people were on the phone. If you would like to use your cell phone there is a telephone room right over here on the side, and if you go in and shut the door or go out into the lobby outside the conference center that would be very helpful.

We ran out of the WiFi brochures but if anyone wants to connect to WiFi the code is F2CAD42307 or you can come to me, I will tell you the code. F2CAD42307. The bathrooms are located across the lobby towards the security screening, make a left, don't go through the card readers, towards the elevators there's a little hallway there and the bathrooms are right there. Fire exits are through the main doors that you came in. Or you can go out the pantry area that's straight back that way to the G Street corridor. In the event of emergency or drill proceed to the building diagonally across the street. Finally, I would like to thank ChoicePoint for providing the coffee and pastries this morning. And now without further delay we will – Oh.

<<AUDIENCE MEMBER

(off mic)

>>KRISTIN COHEN

The list of panelists is on the agenda. So you do have the list of panelists. And as for email addresses –

<<AUDIENCE MEMBER

(off mic)

>>KRISTIN COHEN

If you would like to send an email letting us know that you'd like that, we can contact the panelists and see if that would be okay with them.

<<AUDIENCE MEMBER

(off mic)

>>KRISTIN COHEN

Ok. We will. Are there any other questions? Okay. I'm going turn it back over to Joel Winston who is the moderator for our first panel on upcoming challenges.

>>JOEL WINSTON

Good morning, again. I'm still Joel Winston and we're running a little short on our panelists. Aha. Here we go. We have two out of three. And one on the telephone, Stacy Cannady, missed his flight this morning. It was I guess cancelled or postponed. So we have them through the miracle of modern technology, we in theory have him on the phone here so hopefully it will work. Let me introduce our three panelists and then we'll get started. They'll each be speaking for about 20 minutes.

Stacy Cannady is Product Manager of Security Solutions for Lenovo. He's been in the information technology field for 27 years and has spent the last ten years as a Product Manager specializing in data security and products and services. Mr. Cannady has technical expertise as well as extensive knowledge of the security market. He'll be speaking about Voice over Internet Protocol and mobile payment systems and some of the authentication and security issues they raise.

Second is Hanne Sjursen. Is that close? Hanne is Director of Electronic ID and Payment at Telenor, which is Norway's largest telecommunications company and one of the largest mobile operators worldwide. She joined Telenor 10 years ago after having worked for 14 years with, among others, the World Food Program and the Central Bank of Norway. Since 2004 Hanne has been responsible for the coordination of Telenor's activities connected to electronic identification and electronic payments. And she'll be speaking about her experiences with authentication issues at a telecommunications firm in Norway.

And third we have Yukiko Ko, who is a Policy Advisor at the law firm of Alston and Bird. She advises companies on electronic commerce, related policies and laws, including data protection, Spam control, Adware control and electronic transactions in Asia and Latin America. She has extensive experience in providing intelligence and analyses on e-commerce policies and laws and in identifying key policy makers and law makers for multi-national companies. She'll be speaking about some of the new technologies and how security and authentication issues are being addressed in Japan. So we have got I think we have the world pretty well covered. Stacy, are you with us?

>>STACY CANNADY

Yes, I am. Can you hear me?

>>JOEL WINSTON

We can hear you just fine. We have I guess your power point –

>>STACY CANNADY

Yes.

>>JOEL WINSTON

-- set up. If you would just let me know when you would like the next slide.

>>STACY CANNADY

So I expect you have got the title page up right now?

>>JOEL WINSTON

Correct.

>>STACY CANNADY

Please go to the next page titled most computer products are very insecure. All right. So the topic today is authentication, and I will be talking from that point of view, but let's begin very early in the process for where we can find weaknesses in the -- on the issue of security in general and authentication in particular. Let's consider any software company or for that matter any hardware company in the IT industry. We have companies that build database products, that build operating systems, that build telecommunications gear, but what are they in the business to do? I just said it. They're in the business to build database applications or to build whatever else it is. As a consequence they have hired talent and formed a core body of expertise around what it is they build. If it's not security, then they don't know how to do security. It's as simple as that.

Let's talk about this a little bit more. Software companies, hardware companies, all of these companies have limited resources. It's necessary to constrain available resources in order to ensure profitability of the company. Therefore, it is typically unusual to find someone with security expertise in a company that is not directly related to building security products. Since security is not a core value and not staffed, security is always an after-thought.

And typically what you will find in companies, I see this story again and again, as I watch the market, a corporation builds a fine product that does whatever. It gets out in the marketplace and eventually it comes under attack and it is breached. Well, that's because it does whatever, it doesn't do security. This causes some sort of a scandal or some sort of stir in the marketplace. The customer says I demand security. The response of the corporation is, well, we don't have anybody that can do security but how hard can it be? We'll put a password on it and we'll pick up some sort of encryption and we will call this new release our security release. You'll see the marketing people come out and advertise that this is impregnable security. I have seen this happen just in the last couple of years several times from very notable companies. Within 48 hours the security community has taken this challenge and broken their product, sometimes miserably broken the product.

It's at that point the corporation has to make a decision. They either have to go and hire real security people or they just have to blow it off and go on. So as a customer of these companies, it's necessary for you to keep the pressure on the company. Insist that they hire real security people and do real security. That is, if that's something that's significant to you. If you don't require it, they won't do it.

May I have the next slide, please. All right. This, is even when security software is present we are our own worst enemies. So you have done the right thing, you have beat the snot out of your vendors and they've come out with genuine security features in their products. You have also gone to security vendors and purchased security software from them. You've got it sitting on the shelf. Well, okay. Maybe you installed it.

What's the next problem in the use of these security features? It's us. Buying the technology is never enough. It has to be deployed, it has to be -- it has to be used. It also has to be used correctly. First of all, let's talk about default user IDs and passwords. These are very common in system software and even on PCs. In fact, they are so common that I challenge you to go out to Google at your earliest opportunity and search on the key words "product default password and list." You will be shocked at hundreds, in fact thousands of websites that contain lists of products, vendor of the product, the default user ID that the vendor puts in the product and what the default password is for that product.

If you have any of those products in your environment, I would say that there is a very high likelihood that a default user ID and password for at least one of those products

has been overlooked and is still active in your environment. So that's a problem for your administrators.

Another problem for your administrators is unpatched systems. There are so many security flaws coming out against so many products in the environment that the administrators are desperately challenged to keep up. You have operating system vendors putting out patches as often as one a day under certain circumstances. And never less than one a month. One large patch a month. And there are other vendors who are similarly disposed to putting out patches so your administrators have to know that the patch is out there, acquire the patch, test the patch to make sure it doesn't break anything else because that's a pretty high likelihood too, and assuming that everything works you have to publish the patch throughout this environment. As you might imagine, this is quite a challenge.

Lastly, there is the opportunity for a system to be misconfigured. This happens all the time as well. People are in a hurry. Often the people that are installing the system know nothing about it or very little about it. That means the chance is very high that someone is going to make a mistake during the installation and that mistake creates a security exposure.

Lastly, we ourselves as users are often our own worst enemies because we pick bad passwords. I'm sure that either yesterday or today you've heard at least one person slam passwords, and the justification for slamming passwords is not that there is some inherent weakness in the password method of authentication. Strictly speaking there is no inherent weakness in the system. The weakness is in us. We pick bad passwords. In fact, I would be willing to bet that there are people in here that do something like this. They have an ID that has no password or the password is "password," or the password is some combination or interaction of the first, middle or last name of someone that you love in your immediate family. Could even be your pet. Statistically there is a one-third chance that any individual uses something like that for at least one of his passwords. A one-third chance. Pretty high.

So let's move now on to the next slide, let's consider an example. Let's talk about VoIP technology. VoIP technology, voice over IP, was created by people who wanted to carry this conversation. I'm talking to you over a VoIP connection right now. They wanted to reduce the cost of phone calls by making it possible to carry voice conversations over data networks. That was the design point. Did they deliver? You bet. They have a bunch of nice protocols and nice products that do exactly that.

Do they have any security features in them? No, that's not what the mission was. The mission was – design a way to carry voice over a data network. Did I say security in there? No. Is there security in there? No. All right, fine. So since that's the case, as soon as VoIP began catching up to the marketplace the security people started howling, justifiably so.

So now there is a retrofit action going on as the people who develop the standards are in the process of trying to invent security features to build around the VoIP standards. Are they going to be successful in the first round? History says no. If we look at the evolution of wireless data communication, what we see is the same pattern. Wireless was invented because they wanted to communicate without wires, were they successful? Oh yeah. Did they put security in it? No. So they went back and they tried to retrofit security into the early standards and did they succeed? No. They failed miserably. It took three or four rounds of wireless standards before security was present and effective in the standards. Is that going to happen with VoIP? Why shouldn't it be that way? That's the way history has played out.

All right. So let's move to one other point here. Who cares? Why would anyone attack a VoIP network? Why? For money. That's why all attackers are after data networks at this time.

So let's move on to the next slide, specific hazards with VoIP, and talk about that. Here are three examples of why people are interested in attacking VoIP technology for money. The first is long distance fraud. If you have a VoIP network in your facility, there is a very high chance that there is a default user ID and password in some piece of technology, probably associated with the central VoIP servers. Why? It's built in. That's the way the systems are designed.

If your administrators who are probably data specialists don't know that their voice systems have a default back door installed, they might have left it there. There are bands of criminals that know this and they intentionally try to locate these VoIP systems. They are typically found in mid-size companies, the larger companies usually have a VoIP specialist who knows about this, but mid-size companies don't. The way the mid-size company finds out about it is they get a phone bill that is astronomical. What happened? A hacker's found a dial-in number to their VoIP server. They tested the default back door administrator user ID and password. They found that the defaults were there and what they have done is hijacked that mid-size company's VoIP network and given the number out to people who want to make long distance calls. Most commonly these calls are from the United States or from Europe to India and Pakistan. Those are the most frequent sources and destinations of these calls. The calls almost always occur after hours on weekdays and all weekend long.

So when you check your billing statement at the end of the month you will see tens of thousands of dollars in long distance calls made through your VoIP network during those times. That's what's happened. You need to go to your VoIP server immediately and look for the default ID and password and change them.

Let's talk about overt identity theft. I won't be able to tell but perhaps other moderators on the panel can. People in the audience please raise your hand if you have received a credit card in the mail that had a sticker on it and the sticker said dial 1-800 whatever the number is from your home telephone number in order to activate this credit card. Are there lots of people holding up their hands?

>>JOEL WINSTON

I'd say about 90%.

>>STACY CANNADY

So I drive down your home street and I check the mailboxes and I see one of these. So I take it out and I take it home and I open it up and I see here is a credit card in your name with call from my home number. I know what your name and address is because I found it on the letter on the envelope that this credit card came in. I look in the telephone book and I get your phone number. Now I use free software that I downloaded from the Internet, this is VoIP software that allows me to mask my phone number and make that phone number any number I want it to be. I know what your name is, I know what your address is, I know what your phone number is.

I call the credit card number with your home phone number, listed for caller ID on my VoIP software. The person at the other end picks up the phone and says may I help you? I say I'm you and I'd like to activate my card please. The person at the other end of the credit card company checks caller ID, sees that the phone number is correct, activates the credit card, I sign the back, and you're screwed.

Next, we have hacking VoIP networks to access company data networks. As I said, companies large and small know how to tie up data security, data networks pretty securely. They have been doing this now for over ten years. There are fine products out there, so there is an opportunity for corporations to put genuine security in place on their data networks and they often do. This is a good thing.

What's happened is that the corporations have decided we want VoIP. And they slap the VoIP in because the return on investment is so high. And the IT people, they don't know anything about this VoIP stuff. They do know something now. They know there's no security built into it. And they are running the VoIP on top of their data networks.

As an attacker, I know of a list, actually, a long list of standard attacks that can be used to bridge from a compromised VoIP network into what had been a secure data network. Why would I want to do this? That's where the money is. So those are three examples of how VoIP can be exploited for personal gain at the loss of someone else.

May I have the next slide please? How about another example – Bluetooth. All right. The original Bluetooth specification did make an effort at security. This was security designed by engineers who had no idea what security meant but they figured hey, we're engineers, how hard can it be? So they published their specification, they were proud of the job they had done. The security people saw it. After they got through laughing at the toy security that was built into the specification, they commenced to howl about how miserable it was and how bad it was going to be for all of us.

So, once again, we go through the evolution of toy security to somewhat half-baked security to security which is pretty good. It's good enough for Bluetooth, I think. And that sounds good, right? We have got that solved. So there's real security in place. But then why in the attack community do we have these slang phrases, toothing, Bluetoothing, blue snarfing? This is a hobby activity at this time in the attack community. There are people that engage in these actions to compromise Bluetooth devices. First of all, who cares? Well, look at the picture. Do you have one of those devices? Probably so. If you're a European you bet your life you have one of those devices and you have a whole bunch of other devices that are Bluetooth enabled.

Let's go to the next slide. What is the risk with Bluetooth? Once again, the primary risk associated with Bluetooth is you. You didn't set it up right if you tried to set it up at all. That is almost always the point of attack that attackers are relying on. You did not set it up or you did not set it up correctly. So what does this mean? I'm in an airport waiting area as I was this morning for some time, in fact. I'm in the waiting area, I have nothing to do, so I open up my lap top and plug in a little device. You may know that Bluetooth is supposed to have a range of about ten feet. But with my device and a little antenna on it I have got a range of 200 feet. So that basically makes it possible to pick up everybody in that waiting area. I get a constellation of Bluetooth devices, I start scanning each device to see which one is misconfigured, probably around two-thirds of them are and I engage in what's called a Bluetooth pairing operation.

Once I have paired with it, your Bluetooth device thinks I'm God and it will do anything I tell it to do. If your Bluetooth device is your telephone, I can ask for all the phone numbers that you have in your phone. If your Bluetooth device is your PC, I can ask for any file on your PC. Now, I don't know what phone numbers you have got in your phone and I don't know what data you have on your lap top. Do you want me to find out? And finally, my favorite for Bluetooth attack devices is something called a blue sniper rifle. It's an antenna, a Bluetooth antenna, mounted on a rifle stock which has a range of over a mile.

All right. That's about it. I think -- yes, that's the last slide I have on my presentation. I think I'm right about on time. Are we handling questions now or at the end of the session?

>>JOEL WINSTON

I think we're going to do them at the end.

>>STACY CANNADY

All right. So I'm done. Thanks very much for listening. (Applause.)

>>JOEL WINSTON

Thanks. Ok, Hanne?

>>HANNE SJURSEN

Good morning. Yes that's my presentation. Thanks. Today I'll talk about what we're doing in Norway. What Telenor is doing together with Norwegian banks on electronic IDs on the mobile. I just need some help. I will give a quick overview of the Norwegian market both telecoms and banks to give you some background information to understand why we're doing what we're doing. I'll give the history leading up to our cooperation between Norwegian banks. I'll give you details on the cooperation and outline our challenges and opportunities.

I'll start with the Norwegian telecom market, and we like to say that we're the second most advanced market after Japan. Mobile penetration is higher than 100% as a lot of customers have more than one subscription. In a later survey we cannot find any 15-year-old without a mobile. (Laughter.) Which is really amazing. And our latest research I got last week showed that 85% of ten-year-olds have got a mobile.

Norwegians use their mobile for, of course, SMSs and speech but also since 1999 for mobile payment, mobile commerce, mainly for low value digital goods like logos and ring tones. Mobile internet is used by 700,000 Norwegians every month and that's a total population of 4.8 million. Since internet penetration is very high, 2.9 million people have Internet access and 1.6 million people use internet daily.

The banking industry in Norway. The 140 Norwegian banks all cooperate on delivering payment infrastructure. And that cooperation is organized by the Norwegian banking association. This way working together on infrastructure has given Norwegian bank customers very advanced banking services. And after Iceland no other country has a higher penetration of card payments. Debit Payment System Bank Accept, a Norwegian system, is the most widely used payment method. Norwegians are not very fond of credit card payments yet. In 2005 there were 4.9 million debit cards in Norway with 135 transactions per card per year. In Norway we have got 2.5 million Internet bank customers. Internet banking is very high.

I'll now go through the history leading up to the cooperation between Telenor and Norwegian banks. Very early Telenor saw the need for authentication for mobile payments. We started off with a system where we used the mobile number for authentication and identification for payment. This is -- it's still used. But it's only used for payment for small amounts of digital goods delivered to the mobile and that's because of the underlying cost structure for pre-paid accounts and also because of EU regulation. This method of paying is very easy. There's no registration for the customer. You just form what you want, and then you pay. The amount you pay is deducted from your pre-paid account or added to your invoice.

At Telenor we saw that we needed payment methods for larger amounts and for all types of contacts to get mobile commerce going. Specifically, we needed

authentication methods accepted by Norwegian banks for securing the debit transaction that all Norwegians are very accustomed to. So in 2001 Telenor launched an electronic PKI based ID for mobiles to be used for Telenor customers with a bank account in Norway's largest bank. It was a very secure but extremely user unfriendly solution. And nobody wanted to use it. There's just no Norwegian that wants to go to the post office, show his passport and other form of identification and in addition go through a complicated procedure on his mobile to get an electronic ID. It just doesn't work.

So what we did then, we thought we'll have to work on the usability part. So we went back to the drawing board and made an identification and authentication system based on mobile subscription data in combination with Social Security numbers. And we used this for Visa and MasterCard payments because no way Norwegian banks would accept this kind of authentication for their debit card scheme. So we got a very easy solution to register for, a two-minute process. But it was only for our own customers. So customer uptake was very good. But we only managed to get volume on this for our own services. And mainly for pre-paid top-up. For other services it was not a success. No third party service provider wanted to implement the system because they would only reach Telenor's customers. This was back in 2003.

So we had a mobile commerce system for Telenor customers and Telenor services for payment methods not widely used in the Norwegian market. So we had learned the hard way that to provide our customers with all type of mobile commerce services that could be paid for using Norwegian preferred payment method in an easy way we would need to cooperate with Norwegian banks and the other operators in the market. We also saw at that time back in 2003 that the timing was probably more -- there was better timing to do mobile commerce than back in 2000. What we really saw, that our customers, they think that the most important thing I own is my mobile. At least the ones growing up now, 15-year-olds. They go nowhere without a mobile. They never turn it off. Everybody has a mobile. And it's a personal device. Young Norwegians today, they do not plan. My son he never plans for what he's going to go in the evening, it just happens. He cannot understand why I ask him what are you doing tonight. It's just a strange concept, that question. (Laughter.)

Going back to the 70s, no shops were open after 5. Today shops are open on Sundays. It's very strange, we have this very sort of funny article in the Norwegian papers this summer, interviewing young people shopping on Sundays and paying almost twice the price. And I say why do you do this? Why don't you pay your Saturday dinner on Friday and pay half the price? Oh I don't know. They don't understand the concept of planning. It's something we did back in the '70s. You don't plan anymore. And to pay bills back in the 70s, you went to the bank on your lunch hour in Norway or you got your wife to do it because she was at home.

Now you pay bills on your PC and you want to pay the bills on the mobile. Society is changing and so is consumer behavior. We do not want to plan and we want any time any place anywhere services to make every day life easier and more convenient. That's Norwegian. And to deliver these services to our customers, Telenor will need

mobile commerce solutions for all types of content and payment instruments and efficient and user friendly authentication methods.

With these facts in mind together with the previous learning, we started a discussion with Norwegian banks and Norway's second largest operator in 2005. Negotiations were very difficult, mainly because the bank did not trust Telenor. They thought we'd start a bank and compete with them. To help this we sold our electronic ID company, the one we founded in 2000. We sold it to Norwegian banks to state that we were not going to compete with them on electronic ID. They had delivered electronic bank ID to their customers for a while then and we made clear statements that we were not planning to become a bank.

So in the summer of 2000 we succeeded in closing an agreement with Norwegian banks and Bank ID for mobile. And what is that? Bank ID, it's an electronic identification issued by Norwegian banks. It's a PKI system, the Bank ID PKI card keys are placed on the operator's smart card, SIM card using over the air functionally. This agreement includes all Norwegian banks and the system is open for all Norwegian operators, but only Telenor has joined yet. Norway's second largest operator, NetCom, they have a signed frame agreement but they haven't negotiated the terms, the commercial terms yet. But we think they will.

And in this way banking and payment services will be available by the mobile phone any time and any way and without the use of a token. We have mobile banking services in Norway now to use those you have to bring with you a token, the security token. And that's not -- it doesn't work that way. Norwegians -- they carry their mobile phone and nothing else. It's not going to work if you have a security system where you have to bring a token on the mobile. So Internet bank log on and mobile bank log on will be secured by the mobile Smart Card.

What we're doing is that our industries are combining two customer networks, banks to identify customers with operators, customers with a SIM card. In this way we can deliver that the mobile will be the personal identification and payment device which can be used for secure identification to Internet sites, Internet banking, access to digital TV, access to corporate VPNs, signing of contracts, and then mobile payments. So this will be lots of new business for the banks and for the operators.

What challenges do we see? We haven't made the system yet. We're working on it. And our main challenge is usability for the enrollment process. And we have the previous -- we've tried it before and what happened was that out of hundreds of thousands of customers that were interested we only got 5% of people through the enrollment process. So what we've done now is we've designed a two minute process operated from your Internet bank. So to get the mobile bank ID on to your mobile you have to start inside your Internet bank and then you have to go through a two-minute process and you do not need to change your SIM card so we believe this will be easy enough for our customers. I think if we'd been in a position where our customers had to swap SIM cards, we would not succeed.

Another challenge you see is that we have -- we need all the operators to join in. We have to get the second largest operator joining the system. Then we have to sort of take our own medicine. We have to use Bank ID mobile in our future service development. That's the same for the banks. They have to use it and we, Telenor, have to use it. Then we'll have to manage to sell this functionality to third parties. And to get the Norwegian government to start using bank ID for their services. And that's not been easy. We've not managed to succeed in that yet. And last but not least, banks and operators must manage to cooperate well. That's very essential. We cannot start hitting each other's head.

So to conclude, electronic IDs at least in Norway on the mobile they have to be easy to use and easy to register for and they have to be available for everyone regardless of operator, regardless of bank relationship. And the functionality has to be available for every merchant in the market and it must be possible to use the functionality to secure all types of payments. So to succeed and to get a high security ID out in the market which is also user friendly, I think may be the most difficult thing is that we need to cooperate properly. So that's the Norwegian story. Thank you. (Applause.)

>>YUKIKO KO

Good morning. My name is Yukiko Ko. I'm a Policy Advisor at Alston and Bird. Let me open with a Japanese story for you now. First I would like to thank the FTC for inviting me to this workshop on the cutting edge technology issue, very much intertwined with daily lives of consumers. The focus of my speech today will be on the mobile phone use in my country, Japan, and associated security risks as well as policy and technological responses to the new types of threat in Japan. I hope I can bring you some of the useful hints to consider and prepare for the possibility of forthcoming challenges as a result of technology convergence in the United States.

Let me briefly touch upon the mobile phone use landscape in Japan vis-à-vis that of the United States. In terms of mobile phone penetration we're not that different. Approximately 76% of the entire population uses cell phones both in the United States and Japan. However, 79.5% of the total mobile phone users in Japan access internet via cell phone. While at least 19% of the total mobile phone population access online by mobile phones in the United States. So apparently the Japanese consumers are heavy users of cell phones for online commerce.

Another point to note, which is kind of interesting because Stacy and Hanne pointed out that usability and convenience is very important, it comes first. You've put the wireless and then you put the security next. That trend is more so in Japan because the concept of privacy is not really a well rooted concept in my society. We don't even have a translation for privacy. We just call it simply privacy. (Laughter.)

So that gives you -- that's a really western concept for us. So the emphasis comes more on to convenience, usability, easy to access, rather than protection. Even the

Japanese government is prone to consider more usability first rather than protection. This is not to say that the Japanese government does not care about privacy. They really do. I will explain about the government's initiatives on personal data protection and information security later on.

The Ubiquitous Network Society Plan which is a national initiative aimed at transforming the entire country into the environment with easy connection to networks, any time, anywhere, with anything by anyone by 2010. This is a big theme, a big policy theme in Japan. There are many projects and efforts led by the government and the industry to attain this goal by 2010, what I found of is particular interest to them given high rate of internet connectivity by cell phones in Japan.

What spurred the growth of mobile phone E-commerce in Japan? I think that it's a great competition among the mobile phone carriers due to the unique factors in Japan. Of course the government policy such as introduction of a number portability system, and so on has an effect on competition. But Japan's demography and unique consumer taste, "thumb culture," enhanced the competitive environment in the mobile phone scene. Because the market is already saturated we have limited population, we're not projected to grow any more in terms of population, the wireless phone carriers needed to compete in value-added services to secure more revenue. Also the Japanese consumers have a penchant for very small devices with many multiple functions. I love my cell phones in Japan and my digital camera in Japan because it's so small, light, fashionable and so many functions. I love reading the guide books that you get when you buy a new product. So that's the consumer taste.

As a result, many mobile phones offer unconventional mobile phone services that involve online financial transactions. For example, mobile phone can be train passes you swipe yourself, you purchase of course first, and then it gives you because the phone has RFID technology embedded, you swipe at the entrance of the gate of the station and then you can move in.

Also airplane boarding passes, you're busy, you want to have internet access but there's no -- you don't have lap top. Take out your cell phone, you go online with your cell phone, you purchase and then it gives you a barcode or RFID technology, and that becomes your boarding pass so you go to the gate with your cell phone and swipe in and you go in. Also we download -- well, cell phone becomes a book. You download a novel online and then you see people just reading like this on train or whatever. Also we watch TV. Very useful.

And many people use restaurant search application service by cell phones. I'm no stranger to this. When I'm back in Tokyo when I'm looking for good restaurants I just take out my cell phone, look for good ones, location, price, what kind of cuisine, is it for parties, is it for formal dinners, and it's not just easy access to the whole database but also it gives you discount coupons. (Laughter.) So it's very convenient. You look it and you find this one, you make a reservation and then you get the discount coupon and you give

that coupon, it's actually like a barcode, and give it to the restaurant. So you get not just a pleasant meal but reasonable dining deals, so I love it.

Cell phones are used as electronic wallets. For instance, some cell phones allow subscribers to use a national electronic card cash network called EDY. E-D-Y, EDY. How it works is that RFID is embedded in the cell phone that transforms the device into a credit or debit card. I think we use more for debit card use. Credit card we don't have a well grounded credit card culture so we prefer to pay in advance, prepay. But that's EDY card. This electronic wallet, the customer swipes the phone against a vending machine -- we're also a vending machine culture. If you have prepaid EDY cash network downloaded in your cell phone, you want just a coke, you swipe your cell phone and you get a coke. Also ATM as well. If you swipe on train tickets dispenser, you can get the ticket if you don't want to buy a pass.

A recent interesting trend in Japan is what we call toilet traders. They're a growing number of mobile phone users that take a restroom break and invest and trade stocks using mobile phones in a very private setting. (Laughter.) I have to say that the high volume of mobile phone use contributes to the recent surge in the number of individual investors in Japan. Now, so much for showing off our mobile phone culture.

Let's move on to some of the risks and threats that we face. All these mobile phone-based services involve some kind of financial transaction. This is why it tends to alert criminals, naturally. That most of the ID theft cases stemming from mobile phones in Japan are caused by lost or stolen cell phones in Japan, so it's more conventional. You lose your device and maybe you get a high bill. So what it tends to be is that instead of storing data in your cell phone you tend to store all the data on the network server. And if you lose your cell phone then you remotely control and delete everything or just shut down. But the data is not lost because it's on the server.

Other type of threats risks include one-click fraud, which is kind of phishing. Criminals send emails to your cell phone and then the consumers will be attracted to click on one button without really looking at this tiny specification of what the service is and you click and then the screen comes up saying that the gangsters will come to your home if you do not pay this amount immediately. And of course that's not true but many consumers get frightened, panic and say okay I just put my bank account and -- so that's a very common fraud case that we see. Although some mobile phone carriers can show applications they can operate on their phones and that is to be able to protect the subscribers from activities like the malware installation, they cannot completely protect the handsets from receiving viruses by emails.

At this moment I have said ID theft cases in Japan are not as sophisticated as in the U.S. but there have been multiple government industry initiatives to prepare for ID theft cases similar in the U.S. to come to the mobile phone scene in Japan especially considering the heavy use of RFID technology and emails that you can attach files.

What are the policy responses? There's a laundry list of legislations available to protect consumers from online fraud including that of by mobile phones. Personal information protection act to specify commercial transactions law, the law on regulation of transmission specific -- specified electronic mail, this is anti-spam law and the act against unjustifiable premiums and misleading representations to name a few. The last law is more like FTC law. These all apply to online mobile phone transactions.

The financial instrument and exchange law which will take effect from April 1st, 2008, this is the financial services agencies law, it's dubbed J Sox because of its similarity to Sarbanes-Oxley law in the US. This law contains information security governance as a part of internal control requirements which is a little different from U.S. Sarbanes Oxley law because it's not specifically written but it's implied in Sarbanes-Oxley law in the U.S. but in Japan it's written. Ministry of Economy and Trade Industry, even though they are not the supervising authority of this law, they created these guidelines for businesses on information security governance. And the law of course applies to mobile phone use at work and off work.

On governmental mobile economy commerce security project, three years ago a coalition of government, industry, research organizations in Japan was formed in order to conduct research on deduction of common platform for higher security on mobile phone networks. This project was funded by the national institute of information communications technology, which is the government center, mobile IT forum which is a consortium of businesses, company called Hitachi, NTT Docomo, (indiscernible), and NEC were the industry participants to this project. In January this year this coalition announced the development of common platform based on PKI authentication for higher security on mobile phone networks.

I think Hanne you emphasized the importance of the cooperation among industry. I remember that 140 banks in Norway, they all collaborate. This is very important to create a very sophisticated security network. This platform will be interoperable among several mobile phone carrier networks. This project aims to set a standard for mobile phone authentication technology and I think the coalition is thinking of bringing this to ITU to demonstrate.

I have explained the policy responses. What have been the technology responses? There are two types of authentication methods that I'm sure is being spurred already in this workshop, they are currently employing authentication R&D in Japan, one, definitely biometrical authentication, in particular finger vein authentication, which measures the patterns of veins in your finger which are inherent physical characteristics. And companies like Hitachi, Fujitsu, NEC and Matsushita are the leading companies on this R&D.

Iris authentication. Iris recognition technology for mobile terminals are underway at this moment. This technology is based on an iris recognition algorithm using standard optical cameras that are equipped in mobile phone terminals.

Multi-factor authentication. One time password authentication system using mobile phones. For example, you have a cell phone that has a token already installed and then you use it with a password. Sometimes a password what we call -- there is a system called J password. Instead of using the standard alphabet we use Japanese character sets that are very complicated. So it's a reverse language barrier. We use the language barrier as -- on our advantage.

To conclude, I think with an increasing number of the use of 3G mobile phones, even though the use of cell phones is inferior in the United States at this moment compared to Japan, the problems I laid out should not be ignored in the U.S., especially considering the pace of technology convergence. You in the United States have already established thumb culture well with your Blackberry and now you use cell phones and I'm sure you will start using online transactions soon I think. And I have to -- I cannot emphasize more the importance of the consumer education and the public-private partnership in developing policies and systems to counter new threats to ID. Consumer education and industry cooperation is I think the other key words. Thank you very much. (Applause.)

>>JOEL WINSTON

Thank you, everybody. Stacy, are you still with us?

>>STACY CANNADY

Yes, I am.

>>JOEL WINSTON

Terrific. I have a few questions then we'll open it up to the audience. Stacy, you talked a lot at the beginning about how businesses perhaps are not proactively building in security and authentication measures as they develop these new technologies that they're frankly more interested in getting the technologies out there and making some money. What can we do, we meaning the government and we meaning American society generally, to change the incentives for businesses to build in security at the outset?

>>STACY CANNADY

As consumers of technology and both government and citizens and commerce, commerce businesses all sit in this category, you need to insist on the presence of effective security built in to the solution, whatever it is. It's not in the interest of a widget company to build security into their widgets, they're in the business of making and selling widgets. So it won't be until the consumer demands that the widget has security features built into it that they will deliver. That's just the way capitalist business operates. So I'm not saying a bad thing about corporations when I make these statements. They're competing in their own capitalistic self-interest so it's important for us to make it in their self-interest to feature security.

In terms of what the government can do, well, you are a powerful buyer. And I think probably the strongest lever that you've got is internal binding guidelines that make sense and deliver a consistent message that widgets that have security will be purchased by the American government and those that don't, won't.

>>JOEL WINSTON

So you think government as a purchaser can be influential?

>>STACY CANNADY

Yes. I think it may be that the government underestimates its power based on its presence in the marketplace as a buyer. We will deliver what you say you want whether we like it or not, because we want to sell to you.

>>JOEL WINSTON

It's interesting because when I speak to business groups I often talk to Chief Privacy Officers or Chief Technology Officers of corporations about how they can change the incentives at their companies to build in more security. And what they often say is well, I can't convince senior management to spend the time or take -- spend the money to do this because there's no return on investment. And that's all they're interested in, return on investment, to which I have taken to saying I think the return on investment is not having your name in the front pages of the USA Today or the New York Times about the latest data breach.

>>STACY CANNADY

They all get born again as soon as that happens to them. So that song changes the instant it affects them personally. For you as the governmental entity, if it's part of the terms and conditions, that I can't sell to you unless I meet this certain security standard in products that I want to sell to you, that's return on investment for me, I can't sell to you unless I step up.

>>JOEL WINSTON

Hanne, I want to ask you and I would like the others to jump in also. Seems to me a critical question here is how much can we expect of consumers versus what the businesses' obligation is to bake in authentication techniques that are effective or security techniques that are effective? There's been a lot of discussion over the past day or so about educating consumers, getting them to change their passwords, to adopt safer practices when they're using these devices. But it seems like there's a limit to what consumers are able or willing to do. How do we bridge that gap?

>>HANNE SJURSEN

What we're doing when we are introducing an electronic ID for everyone is that –

>>JOEL WINSTON

Closer to the microphone please.

>>HANNE SJURSEN

What we're doing -- sorry? Yeah, okay. Sorry. What we're doing when we're introducing an electronic ID is we really are giving people a very secure -- maybe for some applications a too secure way of authenticating them. But that has a cost side of course. What we managed or we think we'll manage is to make something very secure, also very user friendly. So what we think is that we -- if we get -- with the strong mobile usage in Norway and the fact that all Norwegians carry their mobile phone with them always, that we'll just persuade them that this is the way to authenticate themselves, to web services when they're doing mobile commerce so they don't have any other choice.

And I think the security risk with the PKI ID system is of course that if I -- it's a code I have to remember, a four digit code that's the way we're implementing it. Of course if I leave my mobile phone lying around with my four digit code printed on the backside of a mobile, yeah, that's -- that will always be a problem. The people can't remember their codes, but going back to the other system which we have now with user name and passwords and all the different user names and passwords, this will be easier for consumers because it's only one 4 digit code to remember. You have your mobile phone, remember your 4 digit code then you can authenticate yourself.

>>JOEL WINSTON

Yukiko, do you want to add to that?

>>YUKIKO KO

I think it's important to tailor your public education to your consumer taste. Maybe for example you explain the risk, maybe it's very user friendly but you never explain that there will be a little higher risk. Maybe some consumers may tend to take more risk and have more usability. But maybe some consumers can be more privacy conscious and therefore they want to have higher security and they don't care how cumbersome it will be for them to authenticate. So maybe providing some options but also a very unconventional way of doing public education is really word by mouth. It works especially in the school settings, universities, companies, if one person starts talking horror stories it really spreads. And probably lastly, of course, the conventional way for us is to spread the word through mobile phones.

>>JOEL WINSTON

I think the debate that's going on in this country is about what the relative contributions to the solution should be from government, private sector and consumers. I think on the one hand there's some appeal to the idea of the government coming in and saying you must have effective authentication. Here are the different options for how to authenticate. Maybe some of the bank agency rules, while very open-ended and flexible do try to get at this idea of there's a certain minimum level of authentication and security that you have to build in. Then the other end of the spectrum is the government shouldn't be dictating this at all, they should be developing through the market system and ultimately it's going to be the consumers' responsibility to protect themselves.

I sense a lot of frustration out there on the part of the public about these issues. They hear a lot about identity theft, they hear about -- they know -- they've even been victimized themselves or know people who have been victimized. And they're having a lot of information thrown at them about how to protect their data, how to authenticate themselves, memorizing passwords and such. Again, I think the issue is how much can we expect as consumers. Any further thoughts on that? Stacy, any thoughts on that?

>>STACY CANNADY

There has been an evolution in security products that I have observed over the last ten years. Security is still often difficult to do. But security is easier to do today than ever before. And a lot of that has to do with the security companies seeing that -- trying to sell a product that is difficult to use, difficult to install, difficult, difficult, difficult, they don't sell a lot of them. So many security companies have spent a great deal of time and effort making security easier. It's showing an effect. So I think part of the solution to the problem that you are voicing is to encourage security companies and companies that are acquiring security features for their products, for their widgets. Make it as easy as possible. Make it something that's going to happen out of the box. I open the box, turn it on, I start to use it, and the security just happens.

As an educated consumer, yeah it's important to me but I don't really understand all this and I have got other things I need to do and I'm just trusting that it's going to keep -- it's going to protect me. That's often the case in the consumer space and in the end user space. So if that's the attitude we have got to deal with, yes, we can try to do some education, after all, we all understand about basic hygiene and the contribution basic hygiene makes to our health. But there are limits to what we are capable of doing in that regard. Beyond that we rely on products that are safe to use, easy to use and do the job. In the same measure, our IT products need to have the security just there, always there, always on, always protecting us, even if I don't do anything.

>>JOEL WINSTON

Here's a question for all of you. Is there a danger particularly with these new technologies, the VoIPs and Bluetooths, that these problems with authentication and security and the resulting identity theft and other crimes that occur, is there a risk that

consumers are going to be so afraid and so turned off by this process they're just going to pull the covers over their heads and stop using these technologies?

>>STACY CANNADY

This is Stacy – that's already happening in the space. There are surveys that indicate that people are less and less willing, certainly in the United States, to engage in online shopping. For a decade online shopping went up year by year. It's not any more. At least the inflection point has been reached and the rate at which it's going up is declining. The percentage of people who are engaged in online banking, it's about 42% right now, and the growth rate for online banking in the United States is 1% per year visioned to cap at 48 or 49% and the reason is that most of the people beyond that just flat don't trust it.

>>JOEL WINSTON

Hanne, do you want to add to that?

>>HANNE SJURSEN

It's not the situation in Norway. I think Norway, well, it's a naive little country up north and we're not going to stop using these systems. I think it will -- usage will increase. And it's difficult for the hackers and the criminals because Norwegian is not a widely used language. So we have the same excuse. So maybe we are sort of protected by the language, yes.

>>AUDIENCE MEMBER

Nigeria (indiscernible).

>>HANNE SJURSEN

We get funny English letters that we don't understand. (Laughter.)

>>YUKIKO KO

I have to say that the situation in Japan is probably similar to Norway. We will not stop using our cell phones. Probably the usage will increase even though we do know that the risk will increase. I think one way to deal with this issue is of course have strong security measures, strong robust authentication methods but also to have vendors, have some kind of recourse methods for consumers if something happens. So the front end and the back end protection I think we need both. And that would make more consumers comfortable even though something happened. Then they would feel comfortable going through another recourse to recover the financial, physical damage.

>>JOEL WINSTON

That raises one other question I have which is, what is the impact of cultural factors from country to country in coming up with successful authentication or security? It seems like people perhaps in Japan and Norway are more willing to jump through some hoops to protect themselves to use these new technologies because they're so important, whereas perhaps people in this country are less willing to do that. That's just a hypothesis but do you think there are cultural imperatives here? Hanne, do you want to start?

>>HANNE SJURSEN

Yes, I think so but I don't know much about the American society. But what we do know about Norwegians is that we have -- we sort of have a feeling that we have got very little time and we don't want to spend an awful lot of time to register for solutions. So with all we're doing we have to keep in mind it has to be easy to use and easy to register for I think. That might be a cultural difference from the states. I don't know.

>>YUKIKO KO

I think it depends on the person, but in general we Japanese tend to like government created standards. We trust government very much that something created by government, it should be safe and you'll be guaranteed. So if government says that this is what we do, then consumers tend to follow even though it could be cumbersome. Of course, there will always be some kind of criticism or reconsideration, but I think culturally a little different from the U.S. in that sense.

>> JOEL WINSTON

I suspect there's a little bit of skepticism about government solutions in this country but -- I don't know why. (Laughter.) It's a mystery to me. Stacy, do you have any thoughts on this?

>>STACY CANNADY

Yes. Cultural issues do play a role. Often we see differences in how technology is used. If we compare what we've heard today about Japanese use of phones and European use of phones, to how Americans use them, very different. There are some stark similarities though. We all pick bad passwords. Just the way -- that's just the way it is and we can take advantage. I think I heard a comment that in some cases we can take advantage of linguistic differences. However, careful analysis of linguistics indicates that there are only about 100,000 passwords that people will pick regardless of the language that they speak. And if there are no -- if there are poor protections against password cracking it takes very little time to try all of them.

>>JOEL WINSTON

Why don't we open it up to the audience now. We have got microphones so if you could raise your hand and introduce yourself, why don't we start here.

>>AUDIENCE MEMBER

I'm John (indiscernible) from Hampshire Research. Can we go upstream a little bit in the process whereby an account or a device is authorized, what kind of standards are utilized when a person presents? Is there a national ID number that is the basis of the account that's created in your countries? And if not, does it apply to other systems as opposed to this communication system? Both Hanne and Yukiko, please.

>>HANNE SJURSEN

To get an electronic ID from the Norwegian banks, you have to go with your passport when you establish your banking relationship. So when that -- when you're 18, you go and get an account and you bring your passport.

>>AUDIENCE MEMBER

When does somebody get a passport?

>>HANNE SJURSEN

You get a passport when you want to travel. We do not have a national identity card in Norway. We have a Social Security number system.

>>YUKIKO KO

In Japan we also do not have national ID. We have driver's license numbers but those are not really widely used. What we do is that when you apply for this kind of ID password for banking they use more comprehensive information -- where you live, which company you work for. In Japan we try to identify person within the community and you identify, not as individual but more of how you are associated with the community. So that's how we tend to define ID.

>>JOEL WINSTON

Other questions over there?

>>AUDIENCE MEMBER

My name is John Carlson with the Financial Services Round Table. I was really intrigued about some of the challenges you found in Norway in terms of the collaboration with your company, a cell phone company and with the financial institution so I would be curious if you could mention what are the elements that make a collaboration successful

and what are the fear factors in -- particularly on the banking side in terms of who owns the customer for the long term?

>>HANNE SJURSEN

Trust, building trust, and that's time consuming. We talked for two, three years. We also used the CEO of our company together with the CEO of the new -- the largest Norwegian banks. And the continued sort of -- stating that Telenor is not becoming a bank and also the banks were telling us that they're not becoming service providers in the Norwegian market.

The ownership of customers, that's a discussion that if you sort of start to discuss that you're in great trouble. It's not a discussion that you can sort of conclude on. So what we said that we would together deliver services -- services based on electronic ID to the Norwegian market, and that's an interesting discussion, not who owns the customers. But lots of people wanted to make that discussion. I had hard time just getting them to go away. Yeah. But I think senior involvement and our CEO stating I want to do this, I want to do this together, we're not going to become a bank. That's important.

>>AUDIENCE MEMBER

Are there antitrust concerns that come up in these discussions?

>>HANNE SJURSEN

What do you mean by trusting…?

>>AUDIENCE MEMBER

Antitrust.

>>HANNE SJURSEN

Ah antitrust. Of course. Yeah. We have a large process with that, but it's all okay, so yeah.

>>JOEL WINSTON

Yeah.

>>AUDIENCE MEMBER

Stacy, I want to direct it to you because you raised the subject and it has to do with the whole security point and with regard to the private sector. My name is George (indiscernible) with the Delaware Credit Union League, but I'm a former CEO of a reinsurance company and the last thing I think any CEO in the world wants to do is get

up and announce 3 million customers were compromised last night because they're going to be heading to the door and the revenues are going to drop and that's what I have been concentrating on for my contract. Are you -- I'm at the point where I'm saying that really the security element is totally outside of the market stuff. It just is not a market incentive. It's in the category, yeah it's leprosy but I may never get leprosy and I got a lot of other things to work on with regard to budget and objectives of revenue and customers. Are you ready to move to that area and say that perhaps government has to put in the curbstones? And is it possible in the security area or -- excuse me, the technological area for the future that those curve stones could be continually moved forward by government? Because I don't see any other incentive within the private side or the revenue and marketing side in order to come up with and make the security part. But it's devastating if I get that leprosy and I have to announce that 20 million customers were compromised last night. And I'll take anything from Hanne and Yukiko on the same matter.

>>STACY CANNADY

I think I'll stick to my guns for a least a while longer on this issue. We're in a capitalist society and corporations make decisions based on money. As a consumer of security technology you're in a situation where if your security technology fails you, there are dire consequences. You have established that. You can express that to your vendors in service level agreements and in selection of partners and in other ways that can influence the vendor behavior. If you're relying on a database for your application, for example, it is possible for you to place requirements on which vendor you choose and on the chosen vendor for security performance in that regard. Your insistence and the insistence of others in your position will modify the behavior of corporations. We have seen that and it can take time, maybe you don't have time. But I still think that voting with your dollars is a powerful incentive.

If you're going to influence with the lever of policy, then you're going to have to be very artful in the construction of your policy so that the policy can endure in spite of the evolution of technology. So for example, if the policy says, this technology is what you must use to provide security, that's almost guaranteed to fail after 18 months, the next generation of computing technology. If on the other hand, the policy reads, you must use a NIST, a National Institute of Science and Technology, approved encryption algorithm for encrypting your data, that's much more interesting. So policy can work but you better be really careful in how you construct it.

>>JOEL WINSTON

Other questions?

>>AUDIENCE MEMBER

I'm Richard Dick with You Take Control. First of all I just want to comment about this last gentleman's statement. All I can say is if your business is on the front of

the Washington Post, you're toast. That's it. It's over. And if you don't understand that, if you don't understand what's at risk, then I'm just feeling sorry for any businessman who doesn't really understand that. We are so vulnerable today. I come out of the healthcare space. Healthcare is running naked. I mean, just flat naked. The emperor has no clothes and doesn't know it. It's just amazing where we're at in healthcare.

I want to ask, though, about, I didn't hear hardly anything about FIPS 140-certified 2 technologies for VoIP. I didn't hear anything much about second factor authentications and different approaches being used with cell phones in that regard. And I'm wondering if any of the panel have any comments on either of those.

>>STACY CANNADY

I can comment on FIPS 140 for VoIP. The only institution that cares at all about FIPS 140 is the US Government. Technology providers who are aimed at the commercial space won't apply that to their standards, to their products. For FIPS 140 for VoIP going to the government, if I'm a VoIP provider and I have no encryption that I don't -- I'm not subject to FIPS 140. So that's my first ploy, to try and offer unencrypted channels to the government since there's kind of a catch 22.

As a government buyer, if you're looking at a product that's going to give you an ROI and it has security in it then there's no standards that apply, then you can buy it. If there is encryption present in it, then you cannot buy it unless it's FIPS 140. That takes time. Sometimes years to get through. So here is -- this is why I was touching on a point if you're going to use policy as a lever to control industry, you need to be really smart on how that policy works. FIPS 140 was designed in the 70s before any of this was dreamed of. And there are shortcomings that show because of that. Now, what was the second part of that question?

>>AUDIENCE MEMBER

Whether or not FIPS 140 and then the second factor authentication.

>>STACY CANNADY

Multi-factor authentication is a very powerful tool in terms of making identity theft much more difficult to accomplish. Yes, I choose bad passwords. We've already established that I and everybody else choose bad passwords. But if I pick a password even if it's bad and use a fingerprint or Smart Card or something like that, things are a lot tougher for the attacker and so I'm a big fan of multi-factor authentication. At Lenovo, I'm the one that drove a fingerprint into the Thinkpad PC for just that reason.

>>JOEL WINSTON

Yukiko or Hanne, you want to comment?

>>YUKIKO KO

In terms of the last question, I briefly touched upon biometric authentication. Multi-factor authentication may be the most robust way is to -- just a fingerprint is also risk to forging so that's why we in Japan try to do R&D on the finger patterns of the vein inside and then you combine with one time passwords and J passwords. The language one. So we have in theory it's very robust. But I haven't seen all those features combined in one because of the user friendly issue that Hanne explained.

>>JOEL WINSTON

We have time for maybe one or two more. Way in the back.

>>AUDIENCE MEMBER

(indiscernible). We seem to be looking very much at the high end of security and authentication here rather than authentication in general and I think that's important to note in that if you look at government mandates and the history, if you get it wrong you look -- sorry, you get it right, you look like a genius. If you get it wrong or just slightly wrong, and here I -- Germany's introduction of ISDN, an enormous push for ISDN to every home, 15 years ago that was being hailed as a master stroke genius. There aren't that many people who are thinking that ISDN is a stroke of genius any more. So when governments get involved in particular technologies, there's a real problem of getting it wrong.

And in particular, you have to beware of geeks bearing gifts (laughter) in that there is a tendency of some of my colleagues to be somewhat technology-driven rather than consumer driven. The thing that really strikes me about the two examples that we have here from Norway and Japan is that they're successful precisely because they are so absolutely uncompromisingly consumer-driven and driven to the consumer's business needs. They're not driven by a let's deploy a particular technology.

>>JOEL WINSTON

I think we now have our theme sentence for the workshop, beware of geeks bearing gifts. Terrific. Last one back there.

>>AUDIENCE MEMBER

I'm with the government, the Commerce Department, Robin Layton, so I'm very interested in the government angle of how we should be involved. And one thing that occurs to me is that the -- at least from what I work on, the internet, is a -- becoming a fundamental communications structure now. An infrastructure so to speak. And with our roads, our transportation, we in the government say you have to have driver's licenses and you have to have insurance. I just wonder, but we don't specify, for example, which

insurance company you need to use, we specify a minimum level of protection that you need to have, but not the maximum.

I'm interested in exploring the role of government. I think I was hearing those gentlemen say that you know, government needs to establish standards through its purchasing policies. Then he was talking about if you're going to establish a policy specifying NIST standards which would evolve over time. So I guess my question is, is it the role of government if there's not enough incentive? I understand that's a point of debate in the private sector to employ sufficient security, is it the role of government to say you must have, if you're going to roll out the service over the Internet, you need to have protection for others just like you need to make sure that somebody can drive or that somebody has insurance in case you hit them? Is there a role for government without specifying a particular standard because I think -- or a particular technology -- because I think we all know that that's not a go proposition. But is there a role for government here in setting some kind of level? And maybe there is, maybe there's not. I mean we're very market sector driven here. But what I'm hearing is this maybe a place where we're seeing some market failure.

>>JOEL WINSTON

I think we're going to be talking about this at the next panel but it's a good segue. We're out of time. We're going to go to a break now but please thank our panelists for a terrific job. (Applause.) Stacy, you can hang up now.

>>STACY CANNADY

You bet. Thank you very much.