FEDERAL TRADE COMMISSION

PUBLIC WORKSHOP:

TECHNOLOGIES FOR PROTECTING PERSONAL INFORMATION:

THE CONSUMER EXPERIENCE

Wednesday, May 14, 2003

7:30 a.m.

Federal Trade Commission

Conference Center

601 New Jersey Avenue, N.W.

Washington, D.C.

For The Record, Inc.
Waldorf, Maryland
(301)870-8025

FEDERAL TRADE COMMISSION

I N D E X

P R O C E E D I N G S

- - - - -

WELCOMING REMARKS

MS. LEVIN: Good morning. Welcome to the Federal Trade Commission's public workshop on "Technologies for Protecting Personal Information: The Consumer Experience." This is a first day of a two-day program. I hope you will return on June 4th to explore the business experience.

My name is Toby Levin. I am an attorney in the Division of Financial Practices, and in addition to being one of the moderators for today, I have the extended duty of making just a few administrative announcements.

First of all, I want to just point you to the exits that are behind you. And know that if, in the unlikely event there is an emergency of any sort, we will get back to you from the podium with the appropriate information, but just make you aware that there are exits behind you.

Secondly, please wear your badges throughout the day. If you exit the building for any reason, you will have to return through security, even if you have your badges on. So we recommend that you stay close by. We have refreshments for you for the morning here. And keep your badges on at all times.

And secondly, here is your first test, to see how much of a technologist you really are. If you have a cell phone, please turn it off now. That will make the program more enjoyable for all of us.

Okay. With that, it's my pleasure to introduce Howard Beales, the Director of the Bureau of Consumer Protection.

MR. BEALES: Thank you, Toby. I am actually here as a stand-in for Chairman Muris. As we begin a workshop about technology, it's perhaps useful to understand the limits of technology, because Chairman Muris was supposed to be here by videotape, but instead, here I am with Chairman Muris's remarks.

Usually I would have to say that the views are my own, and not those of the Commission or any commissioner, but I guess today they are the views of the chairman, and not of any other commissioner or the staff.

But I want to welcome you, on Chairman Muris's behalf, to the first day of the FTC's Public Workshop on Technologies for Protecting Personal Information. Although the chairman couldn't be with you in person, technology was supposed to enable him to share with you his strong interest in this forum, and his thanks to the participants who have come to the Commission to share their expertise and perspectives.

I also want to thank everyone in the audience, whom we hope will carry back with them a better understanding of the issues that frame today's full agenda.

This is the latest in a series of FTC workshops designed to explore the wide range of privacy issues affecting consumers. Just two weeks ago, we held a highly successful forum to examine the many challenges presented by spam. Today, we turn to another topic of interest in the privacy community: what role technology plays in helping consumers and businesses protect consumer information.

We have heard a lot about the promise of technology for protecting privacy. We want to look more closely at whether, and to what extent, consumers and businesses are using these technologies. We will examine technologies that are available to both consumers and businesses.

The session today will focus on consumer technologies, and our June 4th session will focus on business technologies. During both sessions, we will consider technologies designed to manage consumer information, including technologies such as P3P, designed to honor consumer privacy preferences.

We will also evaluate technologies designed to

keep consumer information secure. As part of the discussion of security technologies, we also plan to examine whether there have been advances in information security since our workshop on this topic last year.

Our goal is more than listing the available technology. We want to explore the potential and limits of technology for both consumers and businesses. Have privacy technologies, including those designed to keep information secure, succeeded in the marketplace? Why, or why not? What does research on consumer behavior tell us about how consumers will likely use these technologies? Are certain types of consumer technologies more likely to succeed in the market than others?

For businesses, what role does technology play, as opposed to policies and practices? What challenges can and cannot be addressed by technology?

Today's workshop, in conjunction with the one on June 4th, should shed some light on these questions. It should give us greater understanding of the role of technology in this important area. We have, today, some of the finest researchers and technologists in the field. We look forward to your participation, and thank you again for joining us.

And now, it's my pleasure to introduce Commissioner Orson Swindle, who has played a key role in

this workshop, and in our workshop on information security, roughly a year ago. Commissioner Swindle.

COMMISSIONER SWINDLE: Thank you, Howard, and thank you all for being here. Our audience is somewhat smaller and perhaps less confrontational than one we had a couple of weeks ago.

So, you are all the pros in the business, and you're busy trying to find solutions, and we appreciate not only your help in finding those solutions, but in your help and your participation in this conference. And I think, from each other, we should learn a lot of things.

Bob Liscouski is going to be a real treat for you. I just met Bob a couple of days ago. I found him to be pleasant, a pro, and extremely well qualified for the task that he has been assigned, and that's being Assistant Secretary for Infrastructure Protection. That's an extremely large title.

As I said, I found him pleasant, a professional, and qualified. He has had a career in law enforcement, criminal investigation, software development, information management, consulting, and perhaps the most important job he has had in his entire life, it was for Coca Cola, a good George company which I'm familiar with, as the director for information

assurance.

And we all know what a success that is. So it's nice to have a guy walk in to a new job with awesome responsibilities, and have those kind of qualifications.

He understands what we, at the FTC, understand, that this whole concept of protecting the critical infrastructure of this country is a multi-tiered process. It's like a big triangle, and at the bottom of that triangle are 200 or so million consumers in this country. And they are using computers.

So, therefore, they are linked to the other -- the entire structure. They play a role, and if we think in terms of the strong -- the chain being only as strong as its weakest link, we have a lot of potential weakest links out there. It's a target-rich environment, as we know.

And I think, as many of you heard me say in the past, the solutions to these problems that we face are never going to be found. But we're going to solve many problems en route. It's a journey, and not a destination. There will be many leaders along that road, that journey. You are some of them.

And for that, we always need people who can inspire and cajole in government -- cajole those in the private sector to do what they're most capable of doing,

finding the best solutions, as opposed to government coming in and trying to do it itself.

One of the leaders in that effort, on behalf of Secretary Ridge, is going to be Assistant Secretary Robert Liscouski. Bob, thank you very much for coming over.

(Applause.)

MR. LISCOUSKI: You might want to wait until I talk. You might not like my speech, so just hold any kind of applause. Orson, thanks for your invitation to come here this morning. And importantly, also for the opportunity to speak. I think it's real important.

And I think, when I listen to the introduction, it sounds like I can't hold a job, but I think the reality of it is kind of the way I got here this morning. My function at DHS really allows me to understand the connection at the local level.

And when Orson is talking about the foundation, we've got 200 million users out there of computer technology. Long before I ever got involved in the computer world, my law enforcement experience allowed me to recognize the fact that everything we do is local. And while I represent a national strategy for securing cyber space putting your finger on what cyber space is all about is pretty difficult to do.

But when we talk about the connection between a national strategy and the business community, and the ultimate end-user relationship, that's why I go back to my law enforcement experience at the local level. It's all local. It all occurs at the keyboard.

I've got some prepared remarks, and I've got a colleague of mine that's with me this morning that knows that I often never pay attention to them. But I will use them as a framework to kind of work from to allow you to talk.

I want to talk to you about what DHS is doing, and then what our role, not just within federal government, but at the local level, is all about, trying to generate interest and awareness for security, both within the business community and at the consumer level.

So, a lot of my remarks are really going to be geared at the efforts we're engaged in, and particularly with Orson's group at the FTC, to raise the awareness levels at the consumer level.

A little bit about my background. As Orson indicated, I have been in the private sector. And it's very apparent to me that with respect to the private sector, we have the opportunity in the business community of engaging in a way at the consumer level to not just fulfill our responsibilities to ensure we've got the

right business process, and the right technologies, to assure the consumer we can protect their privacy. We have a responsibility to our shareholders to do the right things as a company, to ensure we've got the right competitive advantage to offer to consumers who have a choice.

And I think that's probably where the nexus of the private sector and the consumer really comes, as it's all about choice. The consumer goes to any industry, I don't care if it's a bank or if it's a credit card, online shopping with American Express, or a small retail store that's got an outlet on the web. The more aware consumers are about what their capabilities are in making choices, and how people can protect them from identity theft and fraud, the more apt they are to make choices to go with companies that are capable of providing that assurance that they will protect them from fraud, that they will protect their privacy.

So, that awareness level is really, from my perspective, fundamental to everything we do to allowing consumers to understand that the choices that they make and with whom they do business is going to be a key market driver for the industries, many of which you represent today.

So, let me first give you an understanding

about what we do at DHS, and why it's really important for us.

Post-September 11th, I think there is no question we all understand how fundamentally different the world in which we live is.

The Department of Homeland Security has been created to help us meet the challenges we have within security, not just at the federal level, as I indicated, but also at the home. The homeland is in the backyard, not at these sometimes innocuous federal buildings we live in. It's everywhere.

The Department challenge was to integrate 22 separate agencies into one, taking responsibilities from the Coast Guard, from the Customs Service and INS, other organizations such as NIPC (National Infrastructure Protection Center), the FedCIRC (Federal Computer Incidence Response Center), all into one umbrella, to try to coordinate our response at the national level. And we have been doing that.

And within my directorate, specifically, the Information Analysis and Information Protection directorate, IAIP, we have done that by combining some of those entities, as I indicated. The NIPC, the Critical Infrastructure Assurance Office the CIAO, the FedCIRC, the NCS, which is the National Communications System, the

Energy Security and Assurance Program Office. We have created that.

And the challenge has been fairly daunting, to be quite honest with you. I mean, when I came here from Coke, I saw it as a challenge of starting something up from the first time, an opportunity to potentially have a positive impact.

I wasn't prepared for the enormity of the challenges that we face. If you could imagine working in a very positive way for a dot-com, in the heyday of high investment, high expectations, a lot of activity going on, all the energy of -- and the excitement that goes along with that, that's one of the elements of it. It's also a merger and acquisition, it's also a hostile takeover, in some cases.

We have a lot of work ahead of us to create an organization. And in the context of IAIP, we have not inherited a legacy infrastructure to allow us to be able to work off of. All this is brand new. So I have engaged a significant amount of my time in organizational development, building an organization, trying to bring business processes together, identify the IT requirements, making sure I know what business we're in.

You would think since we're in charge of protecting the homeland, and the 13 critical

infrastructure components, and the 5 key asset areas it should be pretty straightforward. But when you start peeling away that onion, so to speak, you begin to realize how difficult of a job it is.

So, to suggest that we even knew what business we really were in at the end of the day, and we could identify all the business processes that had to support that, would be an assumption -- an incorrect one, because we don't. We are really in the definition stage right now.

And we are creating a culture. This notion of a culture of security that we refer to all the time, also needs organizational culture to be successful. We have to create an identity and a brand around DHS that people recognize and have a significant amount of confidence in when they see it.

And when Secretary Ridge gets up in front of the public, and he says, "Well, listen, we're raising our alert from yellow to orange, but we're telling you that because you need to be more aware of what's going on, and we need your participation."

Well, if you didn't have confidence in what the Department could do, you're not going to have confidence in what the Secretary is doing, because the culture hasn't been created, and the expectations haven't been

delivered upon yet. We have got to create all that, the capability to do that. And public perception and confidence are absolutely key for us to be successful.

So, we're working hard to bring in all the various components we have inherited. We're working hard at establishing the relationships with the private sector and the industry and the consumers and the general public because, as Orson indicated, this is foundational stuff. These are the things we have to do to ingrain the notion of a security culture that we actually have to create within the general public, that they have a responsibility for their own security.

I think no matter how good a government program we have, no matter how strong and how confident Governor Ridge is in addressing the nation, people must accept responsibility to do what they have to do. We can't reach down to them and do it for them. There is no way we can protect every single individual in the United States. If people don't accept what they have to do, they're going to have to suffer the consequences. They have to be responsible for their security.

Now, the government's responsibility in this is that we have to enable them and provide them the right tools and techniques and methodologies to do these things. And again, that's the essence of what we're

trying to do and will discuss with you today.

I want to emphasize cyber security. I know there are members of the press here who have been probably writing about some of the concerns that the industry has expressed about our lack of focus, or our lack of leadership on the cyber security side.

Dick Clark and Howard Schmidt are evangelists in this area. A significant amount of awareness-raising should be attributed to them. They need a lot of credit for what they have done in establishing the National Strategy to Secure Cyber Space.

But it's a strategy. And as most good thinking, it's only good thinking unless it becomes implemented. And our role, as a DHS organization, within the IP infrastructure, architecture, we're creating an organization to step up to the leadership for cyber security.

We're going to implement the national strategy, we're going to put feet to it and actually work on the deliverables. So I'm going to run this as a business -- as best we can, within the government architecture, to do that. Focus on what can we do, what's immediate, what we can deliver. And we're architecting that today.

We're creating a leadership capability within the Department to be both outward facing, to assure the

industry we're doing the right things, as well as on the execution side, to make sure we're actually doing the right things.

So, we're really stepping up to that challenge, we're working with Orson and others in the federal government to bring the programs to fruition.

Let me emphasize the partnership aspect of it. You have heard, probably, that 85 percent of our critical infrastructure is owned by the private sector. That means the government doesn't own it, we buy the things -- we all buy the things -- that are being produced by that critical infrastructure, we all depend upon those things.

So, the government's ability to protect itself and protect the nation, and particularly protect the critical infrastructure, requires that close partnership with the industries which own those infrastructures. And that's where we're working hard to establish them.

You're familiar with the Information Sharing Analysis Centers, the ISACs, the various industry groups that are out there that we're working hard with. Those are the key components that we're using to outreach, and not dictate what has to be done. But more importantly, working in collaboration with the industries, to ensure the right security programs are being done.

But what are we doing for the consumer? Let me

just talk about the real reason we're here. We clearly understand as the online world becomes more ubiquitous to us, the opportunities we have to interact with technology and the Internet, and virtually any commodity we want to buy, we can buy across the Internet. The availability of the technology, both at a personal level and a business level is clearly the things that make this country a great country. No question about that.

At the business level, the biggest challenge I found in the Coca Cola environment was not getting awareness around the need for information security, but it was actually getting people to do the work, and measure the work that was being done. So we could measure -- we had effective programs.

That was a challenge. The challenge in the business world is how much is the right level of security, when do you stop investing -- when the return doesn't become equivalent to the dollars invested? How do you measure those things? And then how do you make sure you've got the right things going on?

We did that through carefully crafted programs relying very heavily upon our CEO, our senior leadership in the company, to ensure that they sent the message out that these things were absolutely critical for us to do.

We had good people, process, and technology

things going on. We weren't doing all those good things all the time, but we engaged in processes by which we could not just create structure, but spread the responsibility for implementing those programs out across the infrastructure.

We've got to do it again, the same thing. The business community has a responsibility to do it, the consumer groups have the responsibility to do it. And we have got to get people to recognize, from an awareness perspective, what the dangers of the online world are.

It hits home to me, not just at the information assurance level, from my responsibilities at Coke. It hits home for me on a daily basis: I'm the father of two teenage kids, two girls, who are online all the time. They're IM'ing, they're chatting with their friends, they're doing their research, they're always exposing themselves on the Internet. And it worries me to death.

I can tell you, as a former cop and homicide detective, there are a lot of bad people out there, and you see how they exploit people. We have a lot of faith in the technology that we use. It's faceless to us when we interact with a monitor we're looking at, we don't see all the potential bad people that are out there, looking to do us harm.

An example is the other day, my daughter, using

IM, you can put an "away" message on the message when you're away from your terminal. So, for instance, you're online, but obviously, you're going to be coming back. So she puts her phone number on the "away" message. My older daughter sees this, and she tries to act like the mother, and of course they get into a fight.

She comes to me and tells me about it, and she says, "I just want to let you know, you know, she's doing this." And so I walk over, sure enough, and I said, "What are you doing?" She goes, "Well, what do you mean? What's the problem?" I said, "Well, let me tell you what the problem is," and I go through this thing, and it's like, I see the eyes roll and everything, and she doesn't quite get it yet, but we have to begin it at that level and earlier.

If we don't start ingraining the understanding of the dangers of what the online world represents, they're never going to grow up to be consumers that are going to engage in the same process with any degree of competence that we can think, as business people, do our consumers know what they should be doing?

So, it's a behavioral change that really needs to be effected. And that's what we, as a Homeland Security Department, working with, again, FTC and others, that we have to do. We absolutely have to do this. It's

not just a big, federal bureaucracy that has to stand up before an audience and say, "You should be doing these things." We have to have practical programs that people can reach out to and engage with.

So -- and how are we doing that? We're doing that in a variety of things. As I keep indicating, collaboratively working with groups like -- with the FTC, working with the National Cyber Security Alliance, the Stay Safe Online Campaign. We have inherited a good program. That was one of the benefits of the resources we have had when we created DHS, was we have inherited that program from NIPC. We're invigorating that.

We want to make sure we get the message out to the absolute common denominator here. Anybody who puts their hands on a keyboard, I don't care if they're a CEO or if they're a kid in the fifth grade doing a research project, they all need to understand it. It all affects them. And that's our responsibility, as a federal government, to put the word out there. And we are working hard to do that.

I am getting away from my prepared remarks, and I don't want to chew up into the time here. I think probably less is more in most public speaking engagements.

So, I think the message I really want to relay

here is the fact that DHS is not this large federal organization that is going to just come up with a lot of good ideas that we're just going to put up on a website someplace and say, "Okay, here is our idea, and it's up to you to do it." We are going to actively engage, we are going to do a lot of outreach with the consumer groups and private sector, to ensure we've got them engaged.

We want to influence the industry to do the right things, we want to talk to the industry leadership about what their responsibility is to have good software out there. You know, Microsoft, I think, is a leader in this area -- talk about trustworthy computing -- and their ability to provide good software out-of-the-box that doesn't default to everything is open, that we have good security defaults when people put operating systems in they don't have to worry about doing all the little switch settings, and what does that mean to me, as a consumer? Am I going to break something by actually going outside the default mode and putting something in a more trusted way?

The industry has a responsibility, the consumers have a responsibility, we have a responsibility. We all have to step up to that. We're going to engage, you will see more outreach, you will see

more practical programs. You will see more standards coming out. As I indicated, it's not about regulating the industry and passing more laws, it's about doing the things and creating the awareness levels at all the right levels, all the dimensions of this group, to ensure we've got the right things going.

I really have departed from my prepared remarks, but I have got to tell you, if I didn't believe we could do this, I wouldn't have taken on the responsibility. I know we can do it. We can do it at a big enterprise level, we can do it at the consumer level.

I want to thank you for the opportunity of addressing you. Orson, good luck to you on your workshop today. I look forward to working with you in the future. So, thank you.

MS. LEVIN: Thank you, Assistant Secretary.

(Applause.)