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.)

PANEL 1: CONSUMER TOOLS FOR MANAGING
THE COLLECTION AND USE OF PERSONAL INFORMATION

MS. LEVIN: We appreciate very much your taking the time out of your busy schedule to come today. Just a couple of more housekeeping announcements before we begin with panel one.

First of all, we will have a brief five-minute question and answer opportunity before the closing of every panel. If you have a question, a specific question you want to address to the panel, we ask that you go to the center mic in the middle aisle, and we will take those questions at the end of each panel.

Secondly, because we're really tight on time, we're going to try and adhere as much as possible to our schedule, and it may mean cutting short some of the breaks, but since we have food right near by, we're hoping that you will just go out, get a quick refreshment, and come back in so that we can resume our panels on schedule.

And then I also want to give a special thank you to our sponsors for the refreshments today, including Ernst & Young, the Internet Security Systems, Microsoft, Comcast, and The SANS Institute. Thank you again.

One more announcement, if you have anything you would like to add to the workshop record, we will keep

the comment period open until June 20th, which will be several weeks after the second session. So, if you have anything you would like to add, we look forward to receiving your comments. Comments will be posted on our Web page, as well.

Okay. With that, let's begin. Panel one is going to address the consumer tools for managing collection use of personal information. We're going to look at technologies past, present, and future, and some of the challenges, barriers, and incentives for those technologies and the role technology can play.

I'm going to quickly introduce our panel. Their bios are in your folders. To my right -- your left -- Stephanie Perrin, with Digital Discretion; Lorrie Cranor, with AT&T Labs; Brian Tretick, with Ernst & Young; Alan Davidson, with the Center for Democracy and Technology; my colleague, James Silver, who will be assisting me today; Marty Abrams, the Center for Information Policy Leadership; Danny Weitzner, World Wide Web Consortium; Ruchika Agrawal, with Electronic Privacy Information Center; Brooks Dobbs, with Double Click; and Philip Reitinger, with Microsoft Corporation.

All right. Stephanie, will you kick off our panel with your historical overview? Stephanie brought with her today from Canada a poster which some of you may

recall from the workshop at the Department of Commerce some years ago which the FTC co-sponsored, regarding technologies. It's nostalgic. I think it's memorabilia that will be extremely valuable in the future. Thank you, Stephanie.

MS. PERRIN: It will go on the record.

MS. LEVIN: We should put this on the record. We will make a slide of it to put in the record.

MS. PERRIN: Thanks very much, Toby.

MS. PERRIN: I would like to just thank the Center for Information Policy at Hunton & Williams for helping me get down here from Montreal.

I have 10 minutes. And if you have counted the slides that you will see in your package, they will probably take me an hour. So I will be trotting through these slides very, very quickly. If you have questions, please save them for the break.

I think my job is to cover a couple of things: a history of the landscape of how PETS evolved -- privacy-enhancing technologies, that is -- some simple definitions, and basically, what do consumers want from a PET? What are the real market drivers that make PETS succeed in the marketplace?

I was the chief privacy officer at Zero-Knowledge Systems for a couple of years, and we had great

privacy-enhancing technologies that did not sell. So I think we can speak about what sells and what doesn't sell. We were in good company back in the dot-com boom years.

As for the slide regarding the coming threats, I'm sure we won't have time to get to it. We can discuss that in the privacy -- in the question period.

I was working in the federal government in Canada for about 21 years on privacy and security and information issues. And we started having workshops such as this on privacy-enhancing technologies in the early 1990s, subsequent to some OECD meetings on the same topic. And part of the tension was that privacy had always been addressed as a legal issue, as something that you legislate. And the legislators were not talking to the technologists.

Now, I come from a technology department in the federal government, and I should add here that I don't speak for them at all, of course, my views are my own. So is this history.

But the problem, of course, was the lawyers would be setting up laws, and demanding certain things that the technology could not deliver. The signaling system was not designed with privacy in mind. So that leads you to two conclusions.

Number one, when you're designing systems, you should be aware of the legal requirements, or the consumer expectations, or the policy expectations, whether it's legislated or not, and that has to enter into the design phase. So, that dialogue between technologists and policy people has to start early.

And secondly, the technology which was viewed as a great threat to the human right of privacy doesn't have to be a great threat. It can also be an enabler and a facilitator. And it's the only way you do good security, so you have to recognize that what can give you security can also be a part of the privacy landscape.

So, at the time, in the 1970s, when privacy legislation arrived, government was seen as the principal threat to privacy. Then we went through a period where the marketplace was seen as the principal threat. I think we're probably getting back to government being seen as the principal threat nowadays, but that's a topic for another day.

The technology was definitely seen as enabling surveillance, and how to make the technology more consumer-friendly, more sensitive to the need of individuals was the push.

We, in Canada, have a very active privacy commissioner in the province of Ontario who has been keen

on PETS since she first started coming to these early workshops. And she released, with the Netherlands privacy commissioner, a ground-breaking report in 1995 on privacy-enhancing technologies, "The Path to Anonymity."

Since then, we have moved away from this concept of anonymity as being fundamental to PETS. But that's how it started. Now, I am going to skip rather quickly through these.

This slide skips over the structural problems that lead you to want to redesign the technology to enable privacy. We had lived through caller ID -- I will speak for a moment about that. Caller ID was mapped out on the world without anybody really thinking seriously about how to suppress, for those who absolutely needed their number suppressed.

And after it hit the marketplace, places like clinics, doctors who were performing abortions, women's centers looking after women who were being protected from domestic violence, police, all kinds of people, came forward and said, "Hey, you can't release my calling number." Then there was a retrofit on the system. Okay, we will do this call block.

And 1-800 numbers, of course, never had the call block, because that's central to the signaling system. We have the same thing now with 911 enablement.

So, there was then a tension. And that tension persists today. Security people tend to want to gather this data. Privacy people tend to want the system to be designed so that it is not captured. And when I say "this data," I mean transactional data that releases information about the individual.

But that was one of the first fights. And the Caller ID blocking was a patch-on. PETS, since then, have been trying to get integrated into the infrastructure earlier. And these are a few examples of some of the reasons why you might want them, copyright management systems being, of course, pretty important right now.

I am going to skip briefly through these. The original PETS that surfaced in the early 1990s tended to focus on anonymity, such as the anonymous electronic cash rolled out for anonymous road tolls.

I'm not sure how the road tolls run here now, now that they're really quite common currency. But there tends to be transactional data gathering. Digicash enabled the money to be peeled off securely and authentically at very high speeds without capturing consumer information.

Anonymous websurfing, certainly Zero-Knowledge was in that category. We had all kinds of encryption

services, which I have to say, how many people use encryption in their e-mail today? Very, very few. And that's after, really, a good 10 years that it's been commonly available on the marketplace. I don't use it myself. Why? It's too hard. Doesn't work. Crashes my system. Anyway, we won't go there. There is another slide on why consumers don't use PETS.

Other tools started to move in and be welcomed as privacy-enhancing technologies. And then, of course, privacy advocates, as is our want, tended to start bickering about what was a PET and what wasn't a PET. I'm not sure that's a profitable dialogue these days. We have got a lot of problems to solve. So we should maybe get on with it.

But I think it is true, for the purposes of definitions and figuring out what you're going to roll out and what you're going to focus on, you have to understand how big a job a tool is doing.

Into this discussion, of course, was the concept of PITS, privacy-invasive technologies. Many security tools, if they have not been designed with privacy in mind, or privacy enablement in mind, tend to be very intrusive. They can be made more privacy friendly. You can encrypt your biometrics, so that it's a one-way function, so that you don't have a giant

database of people's biometric identification.

You can enable them so that all of the communications is securely encrypted, so nobody can lift this stuff off. RF devices should be designed so that you can turn them off, although my betting is they never will be, because if you do that you defeat some of the crime control aspects of them.

I think I have probably about one minute left, right Toby?

MS. LEVIN: We will give you two.

MS. PERRIN: Two? Thanks. Well, I will just skip through here. I'm going to skip what a PET is. I'm going to skip the boom years. You can look at that poster that I brought from the workshop two years ago, and see how many are still alive.

What do people want? It's got to be easy. It has to have no additional consumer burden, no load. People want it for free. They want it bundled with their products. They don't want to be nickeled and dimed to death. And people don't understand the threat and the potential harm. As we heard a second ago, kids don't know they shouldn't put their telephone numbers up on the Internet. They don't know the basics. And that's normal.

I mean, you still have to train your kids not

to talk to strangers in weird places, and that they should be home at night instead of out at 2:00 in the morning. You have to train each generation about IT, and we are really the first generation that's training about IT. So this shouldn't surprise anyone.

But you're not going to sell something if people don't understand why they should use it. And people cannot understand the data flows. In fact, privacy experts, security experts, and information experts can't understand the data flows. So that's one of the hardest things to understand, where the data goes and shows up, and who can access this, how it can be used.

Now, here are the market drivers list, and I would just leave you with this parting thought, that if we want privacy to be ingrained in the system, we've got to create drivers. Legislation is going to start pushing things in the health sector, because there are some strong requirements there for security. Security and privacy ought to go hand in hand, and not be opponents.

Some of this enforcement action is driving it, just at the tort level. Customer trust and damage to brands. Smart companies -- I'm looking at Richard Purcell here, I love to tease him -- but Microsoft eventually realized they had to do something about

security and privacy, and so went forward and started to do it. Brand is important.

And I will just close on this final note. The security benefits of having less personal information is not sufficiently recognized. And with this thrust now for critical infrastructure protection, there is a drive to get more information about who is doing what to whom.

Leaving personal information around ought to be thought of as leaving a bucket of cash, because it's saleable, organized crime is interested in it, the terrorists are interested in it. You want to protect that like cash. So if you can find a way to avoid having it, through a PET, that's a good thing. You can get the bonus of the use of the data, and make it disappear afterwards. That's a great thing.

I will just cursor through. There we are. Thank you very much.

MS. LEVIN: Thanks, Stephanie. Excellent.

(Applause.)

MS. LEVIN: As you have probably already observed, we have included the slide presentation copies in your folders, so that you can review that information, and it helps our presenters to skim through it faster in their oral presentation. But there is a lot of important information in those slides, so -- good foundation.

Ruchika, would you give us a summary of your perspective on what constitutes privacy-enhancing tools?

MS. AGRAWAL: Sure, though I want to start off by giving you an intuition behind PETS. And basically, we use PETS all the time: cash, Metro cards, postage stamps. And the intuition behind it starts with a question of when is data collection absolutely necessary to complete a transaction or a communication?

And so, with that, we start off with defining a framework for PETS, where PETS eliminate or minimize the collection of personally identifiable information. And we have tons of examples.

Stephanie mentioned websurfer anonymizers. Anonymous publication storage services allow speakers, Internet speakers, to publish anonymously, and it respects First Amendment rights. Anonymous remailers allow users to e-mail, or post in user groups anonymously. Blind signatures -- what Stephanie was talking about, one-way functions -- permit a host of transactions without being personally identified. Digital cash, analogous to physical cash, don't leave a trail of personally identifiable information.

Digital tickets authorize -- we can appeal to the real world. An example of this when you go see a movie, a movie ticket authorizes you to see a particular

showing of a movie. And so digital tickets can serve the same function.

Pre-paid smart cards, if done right, they don't have to leave a trail of personally identifiable information, and there is a host of other examples.

We note that PETS are the way to go, and we observe certain characteristics. One I already mentioned, that they limit the collection of personally identifiable information, they enable communication in commerce, the don't facilitate the collection of personally identifiable information, they don't force users to trade -- Internet users -- to trade privacy to participate in commerce or communications, and they don't treat privacy as a business commodity.

We also note that PETS offer a rich area for future research. There is -- as Stephanie already mentioned -- with security, digital rights management, freedom of expression, computerized voting.

And we close with saying that the critical point in the adoption of PETS is to make it less important for users to understand. I mean, and the model we note there is SSL, which is the secure socket layer, which was widely adopted, which was already bundled into your Netscape Navigator, for example. Users don't have to understand it, it's already part of the system. And

that's the key requirement, we think, to the successful adoption of PETS.

MS. LEVIN: Okay. We will come back and talk a little bit more about what's been widely used in the marketplace and what hasn't in just a minute. And we would like to follow up with Ruchika regarding some of the examples you have given.

But, Marty, would you add to what she said, in terms of your views of what constitutes privacy tools?

MR. ABRAMS: Well, I have been given three minutes to say that it's not just about online, it's not just about the collection of information, that there are other basic privacy principles that we need to think about.

To me, the most important is awareness, or transparency, the fact that we can see clearly how information is going to be used, not just that it's being collected, but how it's going to be used, and the protections around that information. And also, that there are technologies that are enhancing parts of what it means to practice good privacy.

For example, in the United States, where accuracy of information is important, we give people rights to access that information, like the Fair Debt Collection Act, Fair Billing Act, Fair Credit Reporting

Act.

And the technologies, actually, that are coming online have facilitated consumers' exercising those rights much more easily. I can go to Citicorp and get a downloading of this month's account, last month's account, the month before, the month before, so I can see if, indeed, there are issues related to the accuracy of that information. And technology has facilitated that.

So, I think that thinking about this as a conference on PETS is probably inappropriate in a world where we need to think about both online and offline privacy. I think we should think about PETS as privacy-enhancing tools, and that they are multiple tools that we can use.

Now, all of these -- you know, I'm not nuts -- all of these things in the electronic world have to be coupled with the appropriate level of security. And we are still working on what it means to have the appropriate level of security.

If I am going to go and download my account information from the Internet, I have to have appropriate levels of security so I can, indeed, gain access to that information safely. But I think we need to think in a broader term than just sort of the traditional definition of PETS that was put on the table by my distinguished

colleagues.

MS. LEVIN: In the examples that Ruchika gave of anonymous tools, and other tools that are in the marketplace, which ones have succeeded and which haven't, and why? Let's see if we can learn more about that. And Alan, if I can throw the ball to you to start us off?

MR. DAVIDSON: I'm not Paula Bruening, by the way, and that's not my pseudonym, either. I'm channeling Paula today, though.

My first project when I was at CDT was working on what I considered sort of the mother of all privacy-enhancing technologies, which was the liberalization of encryption technology, which I think counts as a success in a lot of ways. It was the enabler of a lot of other technologies that we're talking about today.

A few words about P3P, which I'm sure we will talk about more, as well. But I was going to quote -- to paraphrase the sixties rock band, The Monkees, I'm a believer. I think we're still believers.

And P3P is a first step, it's a modest step. People know this, but there are some notable successes, I think particularly in providing transparency in the area of cookies, for example. I mean, there are some notable successes -- the adoption of P3P widely -- is something that we can point to.

There have been disappointments, and there are a lot of lessons learned from the P3P experience. Lorrie Cranor has written about this, others have talked about it. I am sure we will talk about it more, but slow adoption rates, difficulty in terms of users understanding these systems.

There have been disappointments in other places in the market. The anonymizer tools, some of the tools that Stephanie ran through, we have been, frankly, disappointed that they haven't succeeded. And Stephanie gave a nice run-down of some of the market factors that play into that.

I would just say that I guess a bottom line is that we still are back to -- if you ask why this has happened, I would say that we're still back to what we sort of call the holy trinity around our office of privacy, it's technology, it's also industry best practices and self regulation, and baseline regulation.

And together, we need all of those things, because if you look at the question of how -- where the incentives are going to be to adopt these tools, a lot of them come from those other places. It's an iterative process, where the tools create greater visibility, which drives some of these other areas. But at the same time, those other areas may be what drives the tools.

And anyway, it's not a silver bullet, there is not an easy answer. But I think that we would say all three of these things need to be looked at together.

MS. LEVIN: Danny, I'm going to ask you to follow up with that, again, focusing on the issue of what's been adopted and what hasn't, and why.

MR. WEITZNER: Well, I think it was particularly interesting to hear Stephanie give the long list of privacy-enhancing technologies and note that most of them just didn't quite cut it.

And I think the ones that have cut it, even in the areas such as anonymous browsing, I think what's going to make anonymous browsing work is that, more and more, it will become part of the infrastructure. People are figuring out how to offer it for free.

Now, I think anonymous browsing has, in fact, a relatively small place in most people's online life, and that's for two reasons. And I would broaden that to say that I think that minimization, while a critical privacy principle, in the world we live in, I think is the coequal principle of transparency. I think those are the two important principles. And I think to rest too much hope on minimization is, frankly, to ignore many of the real problems we face.

I don't think that there is an either/or here,

but I think there has been a traditional emphasis in the privacy community, frankly, on minimization. And that's understandable for many reasons. But I think that we have to look around us at the world that we're in, and in fact, at the kind of interactions that people want to engage in online.

The gentleman from DHS's daughter who wanted to make her phone number available, now, I'm sure she got a good education in talking to her sister and her father on that subject. But people do actually want to communicate a fair amount about their identity. They want to be found, in many cases, as much as they sometimes don't want to be found.

And we have to accommodate and recognize the fact, as we build these systems, that the production of culture requires the exchange of identity. Commerce requires the exchange of identity. Politics -- we talk about First Amendment rights -- politics requires the exchange of identity. It's certainly vital to have the right to anonymous political speech, but I think we would all agree, if all political speech was anonymous, it wouldn't be worth a whole lot.

So, I think we have to learn how to pay particular attention as we move forward, to notions of transparency.

But I got off, Toby, so I want to come back to what I think -- the kinds of things that I think can work, and don't work. What is clear is, I think, is that individual consumers are not prepared to shell out a lot of money or a lot of time or a lot of attention in order to protect their privacy. Ruchika said, and Stephanie alluded to it, we have this long list of services that were either too expensive or too hard, or just took more than a glimmer of someone's attention to actually use.

And I think that -- so I think that the answer, in general, whether we're talking about the traditional PETS that are about minimization, or whether we're talking about technologies like P3P -- technologies based on P3P -- that enhance user control, that enhance transparency and choice, these have got to be built deeply into the infrastructure.

I have a bias here. The organization I work with is about creating infrastructure standards for the Web. The reason we have put so much energy into P3P is that we believe that if we build the ability to have better transparency into the Web so that it's a baseline feature, so that it's in the major browsers, so that it's more and more in major server products, it will be easy to deploy, that people don't have to spend as much money, they don't have to spend as much time on making it work.

That's going to be the key, is making these services virtually free, at least to the consumer, and widely enough used that it makes business sense to pay attention to them. If we have 10 standards out there about how to do transparency, the cost, both to consumers and to businesses would be overwhelming and they would never get anywhere.

I think the same kind of thing is true when you look at services that enhance minimization, such as online browsing. We have got to develop common standards. We have some very basic encryption standards out there that are important, but we're so far from being able to facilitate a degree of anonymity in browsing that also, for example, facilitates the delivery of the product you actually found and want to buy.

We're so far from that, we could get much closer to that, but it's going to require an awful lot of work on common standards and common approaches. I think we can accomplish a lot, but we have got to make these things, as Ruchika said, virtually invisible, requiring only a glimmer of understanding of users.

MS. LEVIN: Is the fact that it has to be easy to use and inexpensive, or virtually free, mean that consumers don't care about privacy?

MR. WEITZNER: No, I think what it means, very

simply, is that it's a classic problem of externalities. In any given transaction that a consumer engages in -- and this is true online or offline -- the choice you have is whether to spend extra time right now, extra attention, extra resources of yours, give up opportunities that you might have otherwise, in order to gain some intangible -- seemingly intangible -- privacy benefit that's off in the future.

The cost, if you look at it in crass economic terms, of privacy to users, is the long-term profiling goes on, the long-term intrusion. That cost is not evident in an individual transaction. I think that's why we see, in the U.S., with, I don't know, 37 states that offer the opportunity not to use your social security number as your driver's license number, the usage of that option is tiny. It's -- and it's simply because people, I believe, choose -- are not presented with the long-term costs and the long-term implications.

So, we have to, therefore, turn that around a little bit. I think that part of what's so critical about transparency, I would say more than minimization, what's so critical about transparency is that it helps create both the individual awareness of the actual cost of putting your phone number on the IM message, or disclosing your name, or doing whatever else, it helps

the individuals to be aware of the cost.

And I think it also creates a very important social feedback mechanism. People do need to understand, and need to internalize beyond just, you know, guidance from DHS, which will be valuable, but people need to internalize, in a direct way, the costs of disclosing personal information. And it is only with that, and it's only once people understand that, I think, that we will get the kind of regulatory response that Alan discussed, and find the right balance.

People simply are not aware of what's happening, and we need to help that to happen.

MS. LEVIN: Okay, Marty, why don't you --

MR. ABRAMS: I disagree a little bit. We have lots of teachable moments. We all know that consumers are most responsive when they're at the teachable moment.

In my household, the teachable moment came when my son unintentionally brought spyware into the house with music on our home computer. And I think that it's not just about money, it's about the inner -- it's the way software operates together, it's the ease of putting the software on, it's the ease of making the software work.

I can tell you that our system supervisor graduated from high school and went off to college, that

there are multiple advanced degrees in my household, even with him off at college, but none of us could make the software that was supposed to make our computers more secure work the way our household needed the computers to work.

So, it's not just about money --

MR. WEITZNER: I think you could, I think you didn't choose to spend the time.

MR. ABRAMS: Oh, Danny, I'm not an idiot.

MR. WEITZNER: Oh, I know you're not an idiot, that's why I think you could do it.

MR. ABRAMS: Danny, I am not an idiot, my wife is not an idiot. We have a home network with four nodes. That's just the way our household has to work. And I -- you know, I dispute you when you say that between my wife and I, with the amount of time we had to dedicate -- now, sure, we could go and take a class, sure, we could, you know, go off and spend all of our time doing this.

But we need the technology, to be honest, to work the way Richard Purcell has talked about in the past. It needs to work easily, it needs to work. We need to take advantage of those teachable moments. When consumers put software on their computer, it has to work the way a toaster does.

MS. LEVIN: Alan --

MR. ABRAMS: You put the toast in, and it pops up.

MS. LEVIN: But Alan also pointed out the role -- that technology is one piece, and he mentioned the role of best practices, and also a legal framework. Do you need that to couple with technology, or can technology do it alone?

MR. ABRAMS: I have never been opposed to good privacy law, good security law. I say -- I have often said we don't know quite yet how to write that, and we shouldn't write law until we know how to put it in place.

But I go back to the basics, and some of the basics are that people need to -- when they're at that point where they discover the need for a service or product -- and I see security and privacy as a product -- it needs to be easily usable by the consumer. We need to build that into the products, and make that as something that makes the products more marketable.

Sure, we need to govern the way data is collected in certain instances, we need to have an infrastructure, but I think that's a cop out to say that it's the legal infrastructure that gets in the way of solving the problem.

MS. LEVIN: Can we get some comments from others on the panel, who would like to -- Brian?

MR. TRETICK: Yes. I think two of the most prevalent privacy-enabling techniques that are used today are screen names, like your AOL screen name, your MSN screen name, which disguise your true identity, while allowing you to do things and be contacted.

And the other is, I think again, one of the most prevalently used technologies that's privacy-enabling is Internet Explorer 6.0, which, you know, looks at some of the P3P components that we will talk about shortly. But it's there, it's on, and operating.

I think then, two very prevalent tools that business offers, I think the most widely offered tools, are opt ins and opt outs. And while those don't necessarily limit collection, they could limit use and disclosure. So those already exist today. Those aren't necessarily technologies. Technologies have to be there to drive them, but those are there, as well.

MS. LEVIN: Good additions. Alan?

MR. DAVIDSON: I was just going to say, you know, if you look at -- even at these examples that Brian just gave, I think our greatest successes have been where the transaction costs are low, where tools are being built into other products that people are already adopting.

And maybe that tells us something, which is

that maybe the greatest success story, in some ways, of privacy-enhancing tools is its effect on what we're supposed to be talking about later in the day, its affect on architecture, which is the fact that this has made people start to think about how to build privacy enhancement into other products, other tools.

I don't know where you draw the line between what's a -- maybe Stephanie will have an answer for us about where you draw the line between a privacy-enhancing tool and a change in the architecture or a change in the current product.

But if it's true, as Ruchika says, that consumers really need this to be easy -- and I think that that is true -- the best way to make that happen is going to be to change the products that they're already buying. And that's happening.

MS. LEVIN: Lorrie?

MS. CRANOR: Well, one of the problems that we have is that, as technologists, we don't fully know how to build these things so they just work. And I think a panel this afternoon will talk about that some.

SSL is a good example, that it was given that it just works. Well, actually, it only sort of just works. The part about encrypting your data just works. But one of the roles of SSL is it's supposed to

authenticate, it's supposed to make sure that when I go to, say, Amazon, with the idea of giving them my personal information to buy something, it's really going to Amazon and not somebody else who is actually stealing my information. And that part of SSL actually doesn't work unless you're a pretty knowledgeable consumer. And so, that's a problem.

Another quick point is that I think it's important to look beyond just this online environment when looking at PETS, and to look at the design choices in general. Another thing that was brought up was cards and toll systems. Well, you know, in this country, we typically don't have a public debate when we build a toll system as to, well, should we make it an anonymous system or not, you know. Usually there are so many other factors that get in there, and that gets lost.

And you know, a transit system, the D.C. transit system is, more or less, an anonymous card system. The New York one is definitely not. They do the same thing. There is no reason why they had to be built differently, but they were.

MS. LEVIN: Okay. Anyone else want to comment on how to use these tools? Yes, Ruchika?

MS. AGRAWAL: Well, I just wanted to comment on -- I feel that there is consensus up here that the

important thing about PETS is to make it less important for users to understand it. But I notice an inherent contradiction when you compare that with a technology that's supposed to enable user control. I mean, that, to me, is a contradiction, and I was hoping for a resolution of that.

MS. LEVIN: Can you clarify? Are you suggesting that the tools, by definition, need to allow for user control?

MS. AGRAWAL: Well, like, P3P, and I think Danny has a comment, because -- what I mean is P3P is supposed to enable user control. But at the same time, we're acknowledging that an important aspect to successful adoption of these tools is to make it less important for users to understand the tools.

But if you're trying to get the user to use this particular tool to control their transactions, I mean, it's actually making it more important that the user understands it.

MS. LEVIN: Okay.

MR. WEITZNER: I think that there is a distinction, perhaps, between understanding tools at a technical level, and understanding the results you are trying to achieve. If you expect that people are going to use anonymous browsing, they would only use it with

the expectation and understanding that their identity would be shielded in a certain way.

When technologies, computer technologies, or toasters, or anything else, work properly, people understand how to get the results they want, and don't have to think about how they function.

I think, no doubt, we have seen, even in the early evolution of P3P implementations, in fact, a transition towards the, I think, Ruchika, what you cited as the success of the SSL model, that people see that little lock and key, or they don't.

And Lorrie, I think correctly, points out that people may actually impute the wrong meaning to the presence of that key or not, but nevertheless, it provides a degree of assurance. It allows people to make what computer scientists call a kind of a tacit judgement. It's something you see there, you say, "Okay, I'm happy." You don't have to do what Marty's child evidently did, which was to get under the hood and make things work properly.

That's clearly, I think, where we all want to get. I don't think that there is really any contradiction here if you understand that what we're trying to do is enable people to have a certain kind of experience, and give them control over the experience.

Whether that control is in the form of limiting information altogether through anonymous browsing, or it's in the form of making sure that you only provide personal information in certain contexts.

The point is that people need to achieve the result they want without worrying about how it actually happened. That's what technology ought to do for us.

MS. LEVIN: And so, Ruchika, if I'm right, you're saying that consumers need to understand what the technology does for them in order to make some decisions about it, need to have some level of understanding of how to use it, and why use it, but not need to know exactly how it works?

MS. AGRAWAL: Well, I think there are multiple levels here. And I mean, Stephanie mentioned in the beginning that people don't understand data flows. I'm a technologist, and I used to work for a financial firm, and I did all this e-commerce stuff, and I did not understand the data flows.

I mean, people generally don't understand data flows. And the second level is understanding the technology behind it, which is why we keep saying that it's just important that they're built in, like seatbelts are in a car. It's just there and you use it, it's just less important to understand.

MS. LEVIN: That's a perfect segue into our discussion on P3P, which is a technology that is designed to help consumers understand a whole lot of information in a very automated kind of way, and I think bridges that discussion of education and technology, and policy.

And Lorrie Cranor is here to -- I don't know if she will object to my referring to her as one of the mothers of P3P -- but is here to give us an overview on its status. And then we will launch into a discussion about it.

MS. CRANOR: Good morning. I am also going to go rather quickly through my slides, but you can read the details on your own.

P3P, for those of you who are not familiar, is a standard that was developed by the World Wide Web Consortium. And basically, it's a way for websites to take their privacy policies and put them into a computer-readable format. And the idea is that once they are in a computer-readable format, we can build tools for users, typically into a web browser, that will do something useful with that privacy policy information.

I'm going to skip over all the pieces of P3P. What is probably most interesting about P3P, for people who are not familiar, is what you can actually learn from these computer-readable privacy policies, and here is a

list. You can take a look at of some of the main features. There is actually more details under each of these categories.

P3P supports the creation of P3P user agents. And these are software tools that can actually go and read the P3P policies and do something useful for users. I am going to tell you about a few of them that are currently available.

There are P3P user agents that are actually built into the Microsoft Internet Explorer 6 web browser, and the Netscape Navigator 7 web browser. It just comes with those web browsers. Users don't have to do anything to get them.

These browsers basically focus on one aspect of P3P, something called a compact policy, which is used to describe the privacy policies associated with cookies. And when a website tries to set a cookie, these browsers will automatically take a look at the P3P compact policy associated with that cookie, if it has one.

And actually, the default setting on IE6 is that if there is a cookie that's being set by a third party and it doesn't have a P3P compact policy, that cookie gets blocked automatically. Netscape has different default settings, and users can actually adjust those settings.

Another thing that both of these browsers do is they have a way for users to go and get a summary of a website's privacy policy. And this is done by having the browser go and read that computer-readable privacy policy and then translate it back into English. And so, the user gets a privacy policy in a standardized format from both of these browsers.

Now, there is another tool called the AT&T Privacy Bird, which we developed, which is basically an add-on for IE5 and IE6. You can download it for free. It takes a little bit of effort, because the user has to actually go and get it, although it is free.

Basically, what it does is it puts an icon in the corner of the browser window with a little bird that goes and checks the P3P policy at websites, and it changes colors and chirps to indicate whether or not the website's policy matches the preconfigured settings that the user has put into their browser about privacy. It also has a way of getting that English translation of the computer-readable code.

One of the things that we have discovered in the year or so that these tools have been available, is that they don't all provide identical English language translations. And this is something that a number of websites have raised as a big concern that if somebody

comes to my website and they are using Netscape, or they are using IE6, or they're using Privacy Bird, they are seeing slightly different versions of my privacy policy.

And so, I don't have full control over how users are viewing my privacy policy. And so that's something that's been a concern. And the WC3 has a working group now that's working on trying to come up with some guidelines so that we can get some more consistent representations of these policies in languages that users will actually understand.

Just to show you an example, this is what Privacy Bird looks like. You can see the bird icon in the corner. If I click on that bird, I can get the policy summary -- this is the English translation of the privacy policy. This is a site that matches my preferences, it's a green, happy bird.

Sites that don't match -- I don't think anybody could hear the sound effect, but it was an angry sound -- you have this red, angry bird. And again, we can look at exactly what is the translation, and also, we can see the mismatch. At the top of the translation, we indicate why exactly this policy didn't match my privacy preferences.

Okay, I'm going to take you very briefly through some of the studies that we have done on Privacy Bird and P3P, and there are references where, if you want

to go and look up the complete studies.

We did an e-mail survey of Privacy Bird users. At this point, over 30,000 people have downloaded it. We sent out e-mails to those who had opted in to receiving surveys, and asked them questions about Privacy Bird. Overall, the feedback was quite positive.

The biggest complaint that we got was there were too many sites where they couldn't get an indication from the bird as to whether or not it matched those preferences, because those sites weren't P3P-enabled. And obviously, the tool would be much more useful if they were.

An interesting thing that we saw is that these users reported changes in their online behavior as a result of using this tool. They found it useful, they found it was something that they could actually rely on to do something. These are, of course, self-reported numbers, and not a random sample, but there is some indication that at least some people find this to be a useful thing to do.

There also seemed to be some indication that people would really like to be able to use the tool to do comparison shopping, to keep one of the factors in mind besides price, to look at what are their privacy policies?

Another study which we're doing, and we have some preliminary results on, is we have actually -- we give some users who have never used Privacy Bird or IE6's P3P tools before, we give them some training on how to use them. And then we give them some assignments, to go to some actual websites, read the privacy policy, and answer some questions. You know, "Will this site share your e-mail address for marketing," for example. We have them use Privacy Bird, we have them use IE6, and we have them just read the policy and answer the questions. And then we see how long does it take them to do it, how accurate are they in finding the information, and what did they think of the experience?

This has been very informative, and we found that, overall, using the P3P user agents, people are able to find the information much more accurately, and they certainly have a much better feeling about the process. They like using the tools to find the information. They hate reading privacy policies.

We found that there are some problems, particularly with the IE6 user agent, and this is, in part, due to some of the inconsistencies in the user agent. IE6 actually leaves out some of the components of a P3P policy, which actually make it impossible to answer certain questions. And I think these are things that

could easily be fixed in a future version.

We have also found some problems with Privacy Bird, as well, in some particular types of wording problems, and we're going to be making some recommendations to the P3P working group, as far as in their guidelines, how to address these kinds of issues.

Another thing that came up in the course of the study was what were users actually looking for when they read privacy policies. And what we found is similar to what other studies have found. People want to know what are they collecting about me, how is it going to be used, will it be shared, will I get unsolicited marketings as a result, and how can I opt out?

And I put in purple two of these things. These are the two things that I think are really key. When you ask people, you know, "What is really most important," it's -- will it be shared, and will they send me marketing. The "how can I opt out," I put as less important because a lot of users don't even realize that that's a possibility, so they are not even asking that question.

And one of the things we discovered is that the P3P user agents allow people to answer those questions. But what people would really like to see is right at the top of the screen, they just want the answers to those

questions. They don't want to have to look through and find it halfway down.

Another study that we have done -- and we have a report which, hopefully, will be out on the tables outside shortly, as soon as it arrives here -- is we have done a study of P3P adoption at websites. We have tools that can automatically go and survey websites to find out if they have P3P, and to actually analyze those policies.

We looked at 5,800 websites about a week ago, and we found 538 that had P3P policies. The adoption rates are higher. If you look at the top sites, the top 100 sites, it's about 30 percent, and it goes down as you go down to the less popular sites.

And as Brian will show you in his talk, adoption of P3P is increasing, although slowly. We looked at some specific sectors -- government websites, adoption is very low. We expect this will change, once the new regulations take effect.

We also found that adoption rates at children's websites are fairly low, but there are some interesting trends, which you can read about in the study, with children's sites.

One of the most surprising things that we saw was the number of technical errors in these P3P-enabled websites. About a third of them actually had some form

of technical error. About seven percent we categorized as very serious errors, where they were omitting an essential component.

Now, it's actually very common for web standards to have errors. If you look at other types of web standards and studies that have been done you will see that they all have tons of errors. But we think that there may be some more concern about P3P errors, due to the nature of what P3P is actually telling you, that this may be a bigger problem.

There actually is software and services and tools and books available that should help websites solve this problem. And most of them are available for free, but people are not using them.

And just to give you a little bit of a taste of some of the other things that we were able to find from looking at these P3P-enabled websites, is we were able to essentially do the kinds of web sweeps that have been done in the past for these FTC workshops, but we were able to do them very fast. And in the order of a few hours, we could check 500 websites, and find out how many had opt in, how many had opt out, you know, did they provide access, whatever.

And so, you can see just a few of the kinds of statistics that we were able to collect. And there is a

lot more detail in the report.

Just to -- what I want to leave you with here, so you know, P3P has been out officially for about a year. And I think what we have seen is that P3P adoption is steady, that we are seeing, you know, good adoption rates, but we need more. And we need the sites that are adopting P3P to do a better job at getting it right.

You know, it raises some questions, all these errors that we're seeing, is -- do we need some sort of process to actually go and audit these policies? You know, we don't know anything about are they actually accurate, what they're saying. All we are looking for here is technical errors, but the number of technical errors is somewhat concerning.

We also see that there are some P3P software tools that are available for end users. They are readily available. They need some improvements, but I think that there is promise that we will get those improvements.

We are also seeing that users of these very early P3P user agents are already finding them useful. They will find them more useful when there are more sites P3P-enabled, and there are some improvements.

We are also seeing that P3P has had an unexpected result. Besides being part of a user agent, P3P is also something that we can use to assess the state

of website privacy policies through this sort of automated web sweeps.

And finally, I think in the future, what is going to be particularly useful is to get services that make it even easier for web users to use P3P to answer questions they want at the time they need it.

So when I go to a search engine, instead of, finding the site I want, going there, and then finding out they have a bad privacy policy, what if I could tell the quality of the privacy policy from that search results page, and just go directly to the site with the best policy. And so I hope we will see services like that in the future. Thank you.

MS. LEVIN: Thanks, Lorrie.

(Applause.)

MS. LEVIN: Brian, if you could fill us in on the Ernst & Young reviews.

MR. TRETICK: Certainly. Starting back in August of 2002, we collected data on the top 500 web -- most active web domains for U.S. surfers from Comscore Networks, through their media metrics Netscore program. Without the aid of wonderful technology, we plodded through the 500 sites in August, September, October, planning to check on and report on P3P adoption rates on a monthly basis. We decided that the needle wasn't

moving fast enough, so we went to a quarterly basis -- October to January to April -- the April report is out on the information table, and it's available, also, on ey.com/privacy, for download. Also, the past reports are posted on the site.

What we were able to do with the Comscore data, which separated these top 500 domains according to industry, we were able to determine whether they were P3P-enabled, or had the full P3P policy, not just by count, but also by industry.

In August, of the top 100 domains, 24 out of the 100 or 24 percent were P3P-enabled. And that increased into April to 30 percent.

Of the top 500, we start at a lower level, about 16 percent back in August. We believe we're up to around the 20 percent mark for April. If you look at the dashboard, which presented the percentages as speedometers for these 20 categories, the real outliers, the ones who are well below those 20 percent for top 100 -- 30 percent for the top 100, 20 percent for the top 500 -- are government sites, and those are federal sites in the top 500. Those are also state sites, state domains.

With the e-government Act, we would expect to see, when the OMB publishes those criteria, the federal sites, at least, catching up to where industry is and

actually surpassing them.

We also see a significant lack of adoption in education-related domains, and also the auction -- online auction sites. We hope, in the future, to be made obsolete by the software programs that AT&T Research has put together so we can go off and count things in a more automated fashion. Thank you very much.

MS. LEVIN: Thank you. Lorrie mentioned IE6 and the important role Microsoft has played in the implementation of P3P. Philip, can you comment on that, and bring us up to date on what Microsoft is doing for deployment?

MR. REITINGER: Sure. I would like to -- since I didn't have a chance to talk on the last point raised -- one quick point which leads into the IE6 question. I think I heard raging agreement that privacy tools need to be as -- as all of us, I think, who were involved in the crypto-war, the great crypto-war, as Stephanie put it, a nice turn of phrase, of "double-click, easy, fast, and cheap." It's a phrase from Bill Pullis at EDS.

And I think that is happening. Privacy needs to be built into either the architectural products, as Alan put it, or the architecture of the Internet, as Danny put it. And at least on the product side, I think that is happening.

I won't go into details, given time, but certainly on some of the Microsoft products, like Windows Media Player 9, and Office 11, security tabs and privacy tabs are being included in the architecture of products that allow people to protect their privacy.

Another good example, moving to the topic at issue, is P3P. As I think was raised, it's built into Internet Explorer 6 in a manner that examines the compact policy for cookies. But it's also important to recognize, as the discussion of Privacy Bird indicated, that it's actually an extensible architecture. So you can have browser helper objects that are designed by third parties that will also enable privacy, and give users additional choice.

Microsoft is also a big supporter of P3P, not only in IE6, but we have deployed it across our websites. We think it's an important tool for enabling consumers, particularly to have transparency in notice and choice.

The last thing that Microsoft does to support P3P is we encourage our Passport partners to implement P3P on their websites. So, we think it's a great tool, we're committed to it, and we're committed to continuing to support it in its continued development.

MS. LEVIN: Given your experience with your Passport companies, in particular, how easy is it for

them to implement P3P? What's been your experience?

MR. REITINGER: I'm going to have to speak a little bit not from personal knowledge on this, because that's not my main business line. I think when you talk about incentives and disincentives to adoption of P3P, we have already discussed them to some degree. I would sort of group the disincentives into three categories: cost, risk, and control.

Cost is mostly start-up costs, actually setting up the website to do that. I think that is dropping, but it might be perceived to be higher than it actually is.

Risk, all sorts of things that we're going to get to later, with regard to legal concerns -- probably fall into three rough categories. First, what if you have two policies that disagree with one another? The fact that the current P3P vocabulary may be inadequate to express all of the different elements of a privacy policy, and that there might be liabilities associated with that.

And second, the whole question of implementation. How do you actually do that in practice, and what if an implementer doesn't convey your privacy policy perfectly, are you liable for that?

And then the last is control. As was raised, I think, by Lorrie earlier, a user agent might portray a

privacy policy in a different way than the owner of the website would want it to be. And so there is a sense of loss of control.

Counterbalancing those costs, I think, are two big incentives. One, websites don't want to be broken when you look at them with Netscape or Internet Explorer, or one of the other browsers. They want to work.

Second, P3P is really critical for building user trust, by enabling users to more easily understand the privacy policies of the website. And so I think both of those are important things for folks that want to adopt P3P.

MS. LEVIN: Perfect summary. Brooks, how about adding your perspective on the usability and incentives and obstacles?

MR. DOBBS: Yes. I would just like to follow up on the obstacles, and give a little bit of personal experience of something I have seen.

I have an associate I used to work with, and we do lunch about once a month, and we talk about what we have been doing, and I mention P3P all the time -- it's probably one of my favorite lunch topics.

So, I thought I had driven this point home to this friend. And he builds systems for several websites, and they connect data to each other through a cookie.

Nothing nefarious, it's all clients of theirs, but they need to track use across these different websites.

So, he calls me the other day and says -- this is a while ago -- and says, "About 24 percent of my data seems wrong." Then a little bit later, he says, "About 36 percent of my data seems wrong." And it took the second time for me to realize that, those are the adoption rates of IE6. "What you have done is not listen to me at lunch for the past year-and-a-half, and you haven't done any type of P3P implementation to make your cookie work across these sites."

And then what happens is -- he's a technologist, very techno-geek -- and he says, "Where can I get a P3P policy?" I'm, like, "Well, your P3P policy," as Lorrie said, "is a representation of your site's privacy policy.

Then you start to get this merging of the technical folks, the legal folks, and the production folks. And I don't know how many of you have worked in a web production environment, but those folks don't get together in rooms all the time.

And that's one of the real problems with P3P adoption, is that you have really got to get these departments talking to each other to do something that can, in many cases, be very, very simple. But it's very

hard to get that initial dialogue to begin and then, after the initial dialogue has begun, for everyone to feel comfortable with its output.

The legal folks, of course, are very risk averse, and they have never seen this before, and they have no experience with it, and it worries them some because we haven't seen anything come down on P3P. P3P, in the way that it's evaluated most of the time, is just talking about compact policies, which deal in a very small set of tokens -- about 53 tokens.

So, in many ways -- and I'm over-simplifying here -- you've been asked to reduce your privacy policy to 53 tokens. Well, I'm sure we have all seen lawyers drafting privacy policies. I mean, they labor over the wording. So if you tell them, "You're kind of limited to 53 words, and by the way, we have enumerated the definitions of those words pretty clearly," they get a little bit leery of it. And I think that's been a real problem for adoption.

But maybe switching to focus on what I think the great parts about adoption are, is that, increasingly, the web, and what we see as a web page, is more an ingredients list than it is a single entity. I was in a major news site the other day -- and one of the great things we didn't mention about PETS is one of their

goals may not just be to simplify things for end users, but for them to understand that something very complex is happening, and then they can make decisions as to whether, as Marty was saying, whether they want to invest a bunch of time learning about those things, or maybe just trust in the technology.

But as I was saying, web pages are becoming very complicated, and we're seeing specialization. You know, he who provides weather the best is providing the weather map. He who provides ad serving the best might be providing the ad serving. And so we have these pages that are very, very complex and dynamic, and may not even be the same entities collecting information every time you reload the exact same page.

So it's very difficult in a stagnate privacy policy to address that. And it's very difficult for the folks who are in a third party context to make statements about what it is they do.

And that's one of the great pieces about P3P, is that it takes this simple -- this web page -- expands it out to the complex, to all the different entities collecting data, forces those entities to -- painfully, perhaps -- make some statements in some machine-readable formats, and then brings it all back together again by allowing the user to set some baselines, or perhaps

accept the baselines that are in the user agent, and allow some meaningful decisions to be rendered when it would be potentially impossible for an end user to go in and examine all the different data collection and data transfer that's happening as a result of visiting a single entity. And I think that's a very positive application of P3P.

MS. LEVIN: Before we launch into a discussion about the legal implications -- and Danny, I will come back to you, and Marty, for that -- Stephanie, I see you have a point you wanted to make.

MS. PERRIN: One of the things I skipped over in my slides was a basic comparison of this whole issue of information in the economy and in the infrastructure as being very similar to the environmental problem.

We knew after Rachel Carson that we might be having some problems with pesticides. Nobody can track the stuff through the system. And we had organic products on the market in the 1960s -- me, being old, I remember that -- nobody bought them.

And we have a similar phenomenon, I think, with privacy, in that if you wake up and discover you're not getting screened into jobs, you may start to wonder if maybe those postings to anarchist.com are coming back to haunt you. But if you don't understand how the system

works, it takes you a long time to reach that conclusion, right?

And it's the same thing with the environment and pesticides, and heavy metals, and all the rest of it. If you wake up at 55 with colon cancer, you start wondering about all the chicken and beef you have eaten over the last 30, 40, 50 years. And it's too late then.

So, how do you get consumers to understand to make those choices? And I don't want to sit around for the next 50 years watching people gradually figure out that maybe they should be making better information choices. So how do you impel them to do that? Let's talk in the context of P3P.

And my second point, I guess -- and I don't mean to criticize, because I think P3P is a major tour de force, in terms of its technological application -- the problem I see is that it is web focused. And I wonder how many organizations are looking deep into their systems.

I don't care how the web actually collects data. If I'm smart, I'm using an anonymizer anyway, and I don't see why we can't make anonymous browsing a basic fundamental with freedom of association and free speech. I don't see that there is a real driver to collect personal data on web browsing.

But who is going to audit, to see whether, in fact, these web policies are being implemented? Who is going to audit to make sure that the actual policy -- if I go to my bank's website, does their policy that gets read by the P3P engine reflect what they are actually doing? For instance, under the banking laws in Canada, with the Financial Crimes Reporting Act, I am ready to bet it isn't. And that's -- how do we get from the superficial analysis to that deep analysis that we really need to implement privacy?

MS. LEVIN: Before we get to the audit question, let's start off with, first, looking at the legal liability issues. Marty, launch us there, and then, Danny, I know you want to fill in.

MR. ABRAMS: Okay. Just a disclosure. I run a project center that is focused on the whole question of transparency, and how we do notices. It's a highlights notice project. This is what a HIPAA notice looks like when it's in the highlight version, versus the eight pages you see when you go to the doctor.

When you think about notices, you need to think in terms of a package, a layering of notices, and that there are really three parts. One is the complete, long privacy notice of an organization, which is what you base the P3P notice on. And so you take that notice, you look

for the closest approximation within the tokens to create your P3P policy, which is very detailed, but is still based on a close approximation of what was in that longer notice.

And then, when you go to the user agent, the user agent is taking those tokens that are based on an approximation, and then taking another approximation based on the retranslation into English so that it can be in a standard form. We have already heard that with the three user agents that are commonly used today, that you get a different translation in each of those.

So, you are getting further and further away from this complete privacy policy down to this user agent translation. And as Lorrie would say, there is a real possibility for other user agents to appear with a point of view which would then translate in a fashion that takes you even further away from that original privacy policy.

And part of the legal issue here is the liability related to the question of what is the relationship between these different policies, and do I feel comfortable with my liability, based on the translation of a user agent that I had no control over?

So that one of the things that we need to do is really investigate the relationship between these

different types of policies; and the real test there, I believe, is consistency. And in meeting with state attorney generals, and with the Federal Trade Commission, we have stressed the importance of having a discussion about how you measure the consistency between notices.

The other piece of that goes to where do corporations who are implementing P3P, where do they feel comfortable with this final translation of the P3P notice to the consumer?

And the reality is that while they believe P3P -- and that's mostly the companies working in our project, and I'm not speaking for any of them individually -- but they feel more comfortable in having something like a highlights notice that is a snapshot of what they do with information, and would rather see a system where the P3P notice highlights, first, what is the disconnect between your preferences and what the company does with information, but then drives you to the highlights notice that then drives you to the complete notice.

And so, there is a legal issue and then there is a communications issue, and it really rests around the fact that you have different notices that have to be consistent with each other, that have to be based on the actual behavior of an organization, but that there are

issues related to them, and we need to, before we truly have an implementation of transparency systems that work, we need to work out these liability issues.

MS. LEVIN: Maybe before Danny starts, Marty, walk us through, then, what's the sequence, in terms of notices, that consumers would interact with, then, in your scenario?

MR. ABRAMS: Okay. Well, in an offline basis, P3P doesn't really do much in the offline world -- but in the online world where there is a P3P notice, where we have broad adoption, where we have browsers that are actually looking for the P3P notice. The consumer would first interact with the P3P notice and, if everything is fine and dandy, they go off and do their work, if not, they click. And then their user agent would translate the notice into a series of statements.

And then, if they are still interested, they can click on the privacy policy, and if the organization is an organization that has done a highlights notice, then you have the highlights notice, which really gives a snapshot of what the organization does with information. If they don't have a highlights notice, they go to the long, complete notice that is really written by lawyers to limit liability, rather than to facilitate communication.

MS. LEVIN: Okay. That was very helpful. Danny, can you comment on --

MR. WEITZNER: All that?

MS. LEVIN: From your perspective?

(Laughter.)

MS. LEVIN: All that, and more.

MR. WEITZNER: So I want to actually tell one very quick story from the development of P3P by way of comment. Lorrie and Ari Schwartz, who I think I can confirm are certainly parents superior of P3P, did -- you know, we spent, in the process, a huge amount of time -- years and years of people time, and Brooks sweated through this, as well -- trying to work out these questions of what the vocabulary was going to be, what were these terms going to be about, and I just want to tell one very quick story.

There were some in the P3P working group who wanted to be able to use the term "may" in the P3P grammar. P3P is really just a sentence structure. It says, "The site collects information" for this purpose, or that purpose, and gives it to other entities. And Lorrie's slides lay out the grammar more carefully than that.

Some people wanted to say, "The site may collect information," either that it does collect certain

information, it does not collect information, or it may collect information. And of course, those of you who spend a lot of time looking at human-readable privacy policies know that the word "may" is all over the policies.

And the technically-oriented people in the group said, "Well, what does 'may' mean? How do you compute 'may'?" And ultimately, what was decided was that 'may' isn't really a computable term, that either you do collect information or you don't collect information. And that there would be no way for consumers to make intelligent choices about a policy that said, "We might do it," because you have to assume -- you have to either be cautious or incautious.

And that's really just to say that, in some sense -- I appreciate Stephanie's compliment of P3P as a technical tour de force, and I think that that's true in many ways. I actually think P3P is really more a kind of cultural phenomenon for institutions than a technical one.

Clearly, there are technical issues that are hard that you have to work out. But all the issues that Brooks described about actually having to bring together -- I'm looking at Mel Peterson, from Procter & Gamble, who I know has gone through this more than almost anyone

-- what P3P has actually done is force those three groups that Brooks identified -- the technical people, the web production people, and the legal people -- to get together and come up with a consistent statement about what their site actually does.

Now, I think there is a lot of work to be done -- to Stephanie's point -- there is a lot of back-end work to be done about what happens when that information gets past the web barrier to a company's database, do they still follow through, and there is interesting work being done in that area.

But this is really to say that what P3P has precipitated in so many organizations is the need to be consistent about what's being said.

Now, clearly, there is worry from some lawyers -- and as a lawyer, I can say lawyers often get paid to worry for other people -- lawyers do worry that it may not be possible to express a site's privacy policy as clearly in P3P language as it is in human language.

I can say -- and Lorrie can attest to this -- that we spent the better part of the last three years looking for instances of inconsistency, looking for a privacy policy that could not be adequately expressed in P3P. What we do know is that there are realms, such as the mobile web realm, that raises issues such as location

information that have not adequately been described, perhaps, in the P3P vocabulary. But as far as we can tell, no one has come forward with a privacy policy from their website and says, "I can't translate it." No one. And we have asked over and over again.

We want to know, actually. The vocabulary we view as an evolving process. But I think we should be really clear that there are some people who may worry that they can't put in enough caveats to provide protection, that they can't say, "We might do something," or, "We could something," or, "It may" -- or something bad "may" happen, but I think that those people that have actually gone through this process of translating policies have not yet stumbled upon the clear privacy practice that they can't express.

So, that comes to the legal point that I think you want to raise about liability. We had a workshop at the end of last year in November out at AOL to look at experience from -- really, from a technical perspective, mostly, in implementing P3P. Many of you were at that workshop.

And we actually got together a panel of current and former regulators at the federal and the state level in the U.S., Canadian regulators, European regulators, and we asked them all the question, "Are P3P policies

binding on the sites that put them up, as representations that consumers may reasonably rely on?" I'm not stating the FTC standard well, but the universal answer from all these regulators was, "Of course they are."

If a site intends to communicate something to a user, to a customer, about what their privacy practice is, that is every bit as binding on the site as when they state the policy in human terms.

The problem that has been pointed out over and over and over again is what happens if those representations are inconsistent, if the human readable policy says one thing, and the P3P policy says another thing? Lorrie has also pointed out there may be problems that the user agent may render the policy inconsistently.

I think these are all issues we have to sort out, but I think that they're not necessarily as badly sorted out as we might think, or as some people worry about. I think what is really pretty clear is that the vast majority of privacy practices can be expressed in P3P. And when they are expressed, they are equivalent to expressing them in a human-readable policy.

And we should start there as a baseline. Where we find problems and gaps with that, we should deal with them. But I think we should move off of the kind of generalized worry about this, because frankly, it's been

tested in specifics and not found to be as much of a worry as some might think. Where we have specific problems, we should look at them carefully.

MS. LEVIN: Now, Lorrie mentioned a working group. What's the time frame for dealing with the issue of inconsistencies of vocabulary?

(Laughter.)

MS. LEVIN: Everyone is chuckling. Okay, Lorrie?

MS. CRANOR: Well, you know, these consortium working groups are kind of like herding cats. So, we shall see. But our goal is to, within -- I think we said 16 months, and we started the process this spring -- have a complete set of guidelines out.

MS. LEVIN: Marty?

MR. ABRAMS: Again, I think there is general agreement that transparency is incredibly important, that we have to make transparency work, and that there are multiple elements in making transparency work. And I think that there is general agreement that some of these things are well underway, and will be used.

For example, we're beyond saying P3P is a good thing or a bad thing. It is something that is being implemented, and will be implemented more broadly. I think what's important for the record is to make it clear

that there are some issues that do need to be vetted around this whole question of consistency -- completeness -- what happens when there is an agent that the organization doesn't control that renders it different in a fashion that someone thinks is significant. And who is the person who determines what is significant?

So, I think there is a general agreement that these things need to be worked out, they need to be vetted. It just needs to be on the record that the relationship between transparency agents needs to be talked through and vetted and worked through before we get too far down the road.

MS. LEVIN: Okay. Does anyone else wants to comment on the legal liability issue?

(No response.)

MS. LEVIN: Well, it strikes me that we have come to a very good point, which is we have now gone from describing a host of types of technologies to P3P deployment, and we even have a timetable here -- 16 months -- to resolve all the critical issues.

I don't know how many of you know, but the first demonstration that I am aware of, public demonstration of P3P, was here at the FTC back in 1996.

MS. CRANOR: 1997 was the demonstration, it was first talked about in 1996.

MS. LEVIN: So the FTC has really been, I think, very interested in monitoring the progress of P3P, and we appreciate getting the update today. We have a few minutes for questions. If any of you have a question head to the mic right in the middle of the room.

If you will line up, we will try and -- we have about 10 minutes, actually, a little bit longer than we had originally thought, because everyone on this panel was so articulate and concise, we got through quite a lot.

Okay, Mark, I think you may have to turn a button on.

PARTICIPANT: There you are.

MR. LE MAITRE: Passed the test, I think.

MS. LEVIN: Okay, very good.

MR. LE MAITRE: I just wanted to comment on something that Alan said. He gave three drivers. I would like to add another three to the adoption of privacy.

MS. LEVIN: Okay. And if you don't mind giving us your name, just for the record, so that --

MR. LE MAITRE: I'm sorry, Mark Le Maitre. Education, education, and education. And let me give an illustration.

I arrived home about a month ago to find my

wife had purchased a shredder. This was out of character for her, so I asked her why. She said that she had seen an advertisement on television -- and maybe some of you have seen it -- where a man drives into his driveway to find his next door neighbor rifling through his trash, taking away his credit card receipts. And my wife was impacted upon this to go out and buy a shredder to protect our identity from theft.

What I am seeing at this moment in time is an emphasis on the technologies. I am, unashamedly, a technologist, but I also feel for what Marty was saying about getting the education required to actually practice safe information.

If I had a dollar for every time I had to go around and configure somebody's PC in my neighborhood -- and Marty, if you're up for it, I'll happily help you myself; very presumptuous, I realize -- but the tools have to be easier to use. But I think before people will start to try and use them, and really start to give feedback, they need to be educated as to what to expect.

MS. LEVIN: I am happy to say that a lot of today's discussion, particularly in the afternoon, but even beginning with the second panel, will focus on education. And I am glad we need to emphasize it three times, and again three times. We agree, and we will be

looking more and more at that issue throughout the day.

MR. ABRAMS: Toby, could I say something about consumer education? Susan Grant is here, and Susan remembers the good old days when organizations, leadership organizations, spent a great deal of money on consumer education, that there was a lot of money for consumer education at agencies like the Federal Trade Commission, the Federal Reserve banks.

And we actually, in the 1980s, spent, I believe, a lot more on consumer education for both children and adults than we spend today. And I think that the need for being responsive when we reach that teachable moment is greater than it ever has been. Yet, our national expenditures in this area has actually gone down.

MR. LE MAITRE: Let me just say one final thing, that I think that the real problem of a lack of education will be the adoption of such things as the National Do Not Call Register, which I know, Toby, you and I talked about, which is -- if that's the dominant form of preventing this, it's simply to say, "Shut it all off," I think that business and consumers will both lose.

I think that -- certainly since I came here five years ago to the U.S. without an identity of any sort, no social security number, no credit history, I

wasn't on anybody's mailing list, so I have seen a death by 1,000 cuts. And I think that it needs to be repaired over time. That is, education is a progressive thing.

I fear that if we simply jump to the other extreme, and simply shut off through a National Do Not Call or Do Not Spam registry, that everybody loses out.

MS. LEVIN: Alan, do you want to comment, and then we will take the next question?

MR. DAVIDSON: Well, education is clearly extremely important, and going to become even more important when you look at this next generation -- of tools, looking at trusted computing architectures, digital rights management. It's going to become a very complicated space for consumers to try to understand. I think it's going to be very important.

And I didn't mean also for my holy trinity to detract from the importance and elegance of good tools. That is absolutely true. I have been struck as we have had this conversation about some of the collateral benefits that come from the tools.

There are these direct benefits, but this cultural impact that Danny and Brooks talked about, and also the symbolic importance of things like P3P, had a crystallizing effect on people's thinking about building privacy into the architecture and into the products. And

that, I think, are major benefits.

MS. LEVIN: Okay. Next question?

MS. CASMEY: Kristen Casmey, McGraw Hill. My question is about consumers. How many consumers are currently using P3P? Is that something that has been researched? Because I think that as consumers begin using this, it's going to push companies to implement P3P into their websites.

MS. LEVIN: Okay. Lorrie, do you have some data on that?

MS. CRANOR: It's hard to know. We know that there are an awful lot of consumers that have web browsers that have P3P built in. But we don't know how many of them actually look at it.

And in anecdotal evidence, from going and giving talks about it, and saying, "How many of you knew you could get a privacy report in 1996," is that very few of them are using those features.

As far as Privacy Bird, where consumers actually have to go and download it, last time I checked I think there about 35,000 people had found their way to the site and downloaded it. So, the numbers of consumers are fairly small at this point, but there hasn't been a whole lot of outreach to consumers, letting them know that these things are there.

MS. LEVIN: If there is any funding out there for Lorrie to take her show on the road to talk about Privacy Bird, I am sure she would be willing to accept the funding. Thank you for your question. Yes, Brian?

MR. TRETICK: Yes. Still going back to Internet Explorer 6.0, primarily, if you look at the market share of that product, it's got a P3P cookie manager built in, enabled, and it works without you even having to know about it, and makes some automated decisions at the default level.

So, I would say, 40 percent of the browser market in the U.S., 40 million people may be using P3P today and not know it.

MR. WEITZNER: Right. And clearly, most people never will or should have to know they are using P3P. I think Lorrie's point is more to the point. How many people actually use the privacy report function?

I think those are really product marketing issues that product developers are going to have to work out -- what are the features that actually work for people, and how do you build on that?

But we made a decision very early on, after trying to raise consumer awareness about the term P3P, we said, "This is not the marketing strategy," and a number of members pointed this out to us. They had more of a

clue than we did, that this is a piece of infrastructure that's like asking how many people use SSL. The answer is a lot, but if you ask them, they can't tell you.

MS. LEVIN: Can't tell you, yes.

MS. CRANOR: We actually found in our Privacy Bird user study that about a third of our users had never heard of P3P, yet they were using Privacy Bird. And I view that as actually a good thing.

MS. LEVIN: Okay, good. Yes, Fran?

MS. MAIER: Hi, this is Fran Maier, executive director of TRUSTe, and just a couple of comments. We're very excited about P3P. I have been working also with a short notice group. But what we have, on one hand, is P3P, which is something that isn't quite human readable, we have short notice, which isn't quite computer readable. We have to get these things to be more consistent. It is really hard for us.

At TRUSTe, we certify over 1,000 sites. We ask, it's part of our requirements, that there is consistency between any sort of highlights or short notice, P3P and the privacy statement. And it isn't that easy.

And we do have experience with bringing the technology, the production people, the legal people, the marketing people all together in a room. Because again,

at TRUSTe that has to happen. And it is still hard.

So, I would just like to urge you all to -- let's all move together quickly to make these things all work together.

MS. LEVIN: Okay, thank you. Joe?

MR. TUROW: Hi. Joe Turow, University of Pennsylvania. I just had a question about consumer feedback to things like P3P. Is there any facility for a consumer to be able to say, "Well, I like this part of the privacy policy, but the business about third-party pieces on a particular part of the web page is something I don't like, and so I'm not going to come back here until you fix that."

Is there any attempt to really get feedback about what's going to work for most people, or is it just a binary yes/no when you're dealing with a site?

MS. CRANOR: Right now, it's a binary yes/no. There has been a lot of discussion about having a feedback mechanism or negotiation, but that's not in P3P at this point.

MR. DOBBS: And again, you should also realize that a site is not one entity. There can be marginal acceptance. You can accept asset A and not asset B. So the whole site is not viewed holistically. I mean, all the assets that gather information on the site can be

evaluated individually, and preferences applied to the behavior of each.

MR. WEITZNER: Just to underscore the point, there has been lots of discussion in the P3P context, and in the context of other technologies, about how to do some sort of negotiation, some sort of feedback mechanism.

I think Brooks pointed to what there is in P3P now, which is a tacit negotiation at sites. For example, Brooks's friend will find that certain cookies are blocked because they don't match the user's privacy preferences. I don't know where the gentleman is who asked -- oh, there you are.

So, that's not the sort of explicit bargaining type of negotiation that we would think about, but it actually has its effects. And I think in the early implementation of P3P, certainly what we saw, frankly, was lots of sites adjusting their privacy policies so that they would meet the IE6 default level. That was a certain kind of negotiation.

Your question was who was negotiating with whom, but there was a feedback mechanism there. I think in some of the Liberty Alliance technologies, there is an effort to take that negotiation one step further with a more explicit feedback mechanism.

But it's a very hard technical problem, because of the problem of modeling and actual negotiation that happens between individuals, or an individual and a business. It is a hard type of interaction to model, technically.

MS. LEVIN: Okay, thank you. I think we have time, if your question is really brief. I am going to cut off a couple of minutes into the break for the questions, because I think they are important. If you want to take one more?

MR. GRATCHNER: Hi. My name is Rob Gratchner, from Intel Corporation. I just wanted to touch on something real quickly that you talked about with wireless and P3P.

Does P3P work with wireless technology now, and if not, what is the implementation of using P3P with wireless technology that's out there now, and the new technologies that are coming up in the future?

MS. CRANOR: P3P can work with wireless technology. I do not know of a commercially available user agent for a wireless device. I know of some prototypes that have been built in the laboratory. It certainly can work in that context.

There are some extra things that people suggested they might want to do in a wireless

environment, and P3P can be extended to do that, but that hasn't been standardized at this point.

MS. LEVIN: Thank you. We are going to give Stephanie, who kicked off the panel, the last opportunity to talk.

MS. PERRIN: I actually have a question, and you may not want to, when you hear my question. I want to ask, has anybody done a cost benefit analysis of P3P, and how much this has all cost, in terms of development and implementation?

And the reason I ask that -- and I have to declare I spent 10 years of my life working on the framework for, and the drafting of the Canadian baseline privacy legislation -- and I will let you in on a secret. The reason we legislated is it's cheaper.

And I think if you compare the huge amount of effort -- because basically, these processes are the reverse of each other -- P3P has been one of the lead instigators in getting companies to develop policies. They did it so that they could have their website policy.

That means they suddenly discover they have to have policies throughout their organization. Their lawyers have to wake up and figure, in fact, are they doing what they're saying in their policies? So, you have that sort of -- it's a pyramidal flow of activity

and expense.

And in Canada, we very quietly worked on a standard, legislated the standard, then, in fact, you need the same web interface. But it's all exactly backwards. Which is cheaper, I have to ask you, because you still have time to draft legislation. I will come up here and do it really cheap for you.

MS. LEVIN: I am going to end this simply by saying that is a million -- or, I don't know how many million -- dollar question. You have said it at the right place, the Federal Trade Commission. And if any of you would like to file comments with your cost benefit analysis included, of P3P or any technology, please file them by June 20th. Great question.

We will have a 10-minute break. At quarter of, be back in your chairs, ready to go for the next program.

(Applause.)

(A brief recess was taken.)

PANEL 2: CONSUMER TOOLS FOR MANAGING INFORMATION SECURITY

MR. SILVER: Welcome back, everyone. This is panel two, which will focus on the tools that consumers currently have to manage their information security.

We will look at tools that exist both online, and also some tools you may have currently in your pockets right now. We will also examine how consumers can best use these tools.

I will begin by introducing our panelists, starting at stage right over there. Anson Lee is with Symantec Corporation, Mark MacCarthy is with Visa U.S.A., Rich Lloyd is with Dell Inc.

Alan Paller is here from the SANS Institute. My colleague, Loretta Garrison, will be helping me today, from the FTC. Michael Willett is a security and privacy consultant, Larry Clinton is with the Internet Security Alliance.

And Richard Smith is an Internet consultant. He will be leading us off with an overview of the kinds of tools that are currently available online to consumers.

MR. SMITH: Okay. What I want to try to do is give the 10,000 feet view of security products that are available that we use everyday, or many of us use

everyday on our home computers.

In the first session, there was a lot of talk about the use of SSL, or HTTP secure socket layer. It's an example of a technology, I think, which is the most appropriate, in that it just works. It's not something that a user necessarily has to turn on, or specially use in order to get security.

The primary purpose of SSL is to encrypt information that goes between a home computer and a website. So, if you're entering an e-commerce website, and you're buying something, you're providing your name, your address, your credit card numbers and so on, that information is scrambled on transmission.

And the main purpose of SSL is really to prevent eavesdropping, so that if you have got somebody that could intercept, web traffic, they can't look at the stuff. It all looks like gibberish.

And a good example of how easy something could be intercepted is if you're at work and you're buying something at Amazon, your network administrator has -- or other employees could very easily eavesdrop, because you have a shared connection at work.

But there are also problems with eavesdropping on wireless connections and these sorts of things. SSL has been a very successful technology, and overall, has

worked very well. It's an example, I think, of one the best technologies. It's just there, it comes with the product, it comes as part of almost all web browsers, or at least all the ones that, 99 percent of the people of the world use, and it's been a great technology.

Another example of a technology that's built-in, that I like for security, is in Outlook. If we think of a virus problem here, which I will get into next, many of us are very familiar with anti-virus software. It's a kind of software that we buy in order to provide protection.

There is also anti-virus protection, though, in Outlook now. A lot of the viruses that we get, and worms that we get, come through as e-mail attachments. And Outlook, for the last couple of years, will now automatically delete any kind of executable file that comes in as an attachment.

And I find that is a very effective measure. I don't have to worry about keeping an anti-virus software up to date. And it's very transparent. The only problem is if someone -- if a programmer friend sends me an executable and forgets to zip it up, then I have to send him back an e-mail, "try again." But that's just teaching good computing practices, basically.

Another form of protection from viruses, of

course, is anti-virus software. It's probably the most famous kind of security protection out there. The whole idea is that you run a software program in the background on your computer, and as you access files, before you run them, it checks -- or at various times checks -- to see if these are known viruses or worms or Trojan horse programs.

What's good about anti-virus software is that it's, again, an automatic activity that goes on, not something the user has to do, but they do have to install it.

Now, the issue, the problem with anti-virus software is it can't really read the mind of the program, it can't predict if this particular piece of software has malicious intent.

So, with anti-virus software, it's said the way that it works is it has a database of known viruses or worms, and there are thousands or tens of thousands of these programs in the database. And there are little signatures that say, okay, for this particular virus, we know this pattern appears in the program, so if we ever see that in a file, it's most likely an infected file, or an example of a worm. And therefore, we can warn the user of it.

It's kind of insurance policy-type software.

Not everybody gets infected with a virus sent to them. So a lot of things with security, we do have to keep in mind is that they are like insurance. We don't always do it.

Everybody who owns a house has fire insurance, but we don't expect a fire in the house. And a lot of the security aspects that we get into are the same way, that we may, in some sense, not need this software, but we have to have it anyway, just in case.

In terms of new viruses, there are tens of thousands of people out there in the world writing viruses around the world, literally, and so we have, every month, 10,000 new viruses, maybe -- I don't know what the numbers are, maybe Mr. Lee from Symantec could give us a number -- but we need to keep the anti-virus software up to date. And now it's basically on a daily basis.

With the Internet, new viruses are being released and spread within days. So, that's one side of it. The anti-virus question is how we get updates. And through the Internet, it's pretty easy.

How do we get viruses on home PCs? That's just one thing. When we talk about security measures, we want to talk about the threats. And just really briefly here, we get them through e-mail attachments as a primary

method.

And as I mentioned, Outlook will now automatically block certain things so it can provide -- software itself can provide anti-virus protection. We download files from websites. There are security holes that are in web browsers that allow automatic execution of viruses or worms or Trojan horses, inside Word documents -- although that's becoming less prevalent because of some changes that Microsoft has made.

People just love whatever technology is popular through P2P networks -- not to be confused with P3P -- but through song-sharing networks, like Kazaa and Morpheus, and then instant messaging is another way it's becoming popular. Basically, any time you have a network connection and get data this way you're going to get a virus.

Another security technology for home PCs are firewalls. Firewalls began their lives more in the corporate or university settings. We had this concept of a local area network with a whole bunch of computers on it, and you had the evil Internet out here, with all the bad guys trying to break in. And so a firewall is basically a moat, if you will, around -- or a wall around -- that internal network.

So we have trusted computers inside, and you

have untrusted computers on the outside. And a firewall then blocks traffic coming in from that untrusted world into your local area network.

For a home PC, the definition of the firewall has grown, but you can have the same issues. At my household, we have three computer networks. We have one computer for each person, so we have a little local area network. And so we have some trusted computers, and then we have the outside, untrusted world.

And we use what's known as a router box in order to provide the firewall protection. It protects us from any kind of hostile intent that's coming in. And that can be basically hackers trying to break into computers. And the way that they do that is they look for services that are running on unprotected computers, and try to exploit security holes that are in there.

Another thing, though, that the home firewall does is it also looks for what is known as spyware, that is, programs that get loaded on your computer that want to phone out with personal information, or more typically, your web browsing history. And you will get spyware installed on computers through, basically, downloading software, say, like on a Kazaa or Morpheus.

My daughter -- I keep telling her to stop doing this, but she keeps installing Kazaa on her mom's

computer, and so I have to keep cleaning it off the various packages.

What's interesting is anti-virus software, in general, does not look for spyware. So the moral of the solution is see that when a spyware program tries to phone home, the firewall alerts you that somebody is trying to go out. Here you have the trusted computer trying to go out to the untrusted Internet.

And in general, the rule of thumb is that if you're running on a cable modem or DSL connection, a firewall is more important to get, because your computer is going to be online more, and more vulnerable to outsiders trying to break in.

The last kind of software I want to talk about is a spyware detector. As I mentioned, many of the anti-virus software packages today don't look for spyware, and there are many different flavors of it. But there are new packages that are coming out from other companies that work just like anti-virus software that look for signatures, but they look specifically for spyware.

And I have three categories here. One is keyboard sniffers, commercial spyware, and Trojan horses. A keyboard sniffer is a program that simply records all the key strokes that happen on a keyboard, and sends that information off to someone else. There are probably a

couple of dozen packages you can go out and buy, or even download for free, that do this. They are typically sold for one spouse to spy on the other spouse. That's the main market for this software. They are also used sometimes for spying on employees, and so on. But where they really become dangerous is if an outsider uses it to, say, steal credit card numbers, and so on.

And this is how you get around SSL, by the way. If you want to be an eavesdropper, you spy on somebody before data gets encrypted.

So, commercial spyware are packages that provide, for example, pop-up advertising, based on what you're searching for at search engines, that sort of thing, and then you have Trojan horses, which anti-virus software do generally look for.

I will just give you quickly one war story here to sort of wrap it up, of the dangers of keyboard sniffers, which is one-fourth of spyware. A gentleman named Douglas Boudreau at Boston College installed 100 keyboard sniffers around the campus of Boston College, and he was caught.

And he collected personal information on more than 5,000 people in the Boston College community, faculty and students. And he got everything all these people typed on the keyboard all day long. He was just

constantly collecting this information which was being sent off to a server he was running.

And he got account names, password, credit card numbers, PIN numbers, you name it. You know, if you're doing online banking you have to provide your PIN number. So he got it all. You can just imagine -- personal e-mails, just the whole gamut.

A lot of computer crooks, though, don't actually make good criminals. He didn't monetize, if you will, all this information being collected. And he only ended up stealing $2,000. And therefore, when the State of Massachusetts went after him, the state decided not to throw him in the pokey for 20 years, but just put him on probation for a few years. I thought that was a little bit light for the sentence.

But it just shows you some of the dangers here of these kinds of software that are out there, some of the threats that are out there. And when we get smarter criminals out there who are using keyboard sniffers, they could steal, actually, a lot of money. Thank you very much.

(Applause.)

MR. SILVER: Thank you, Richard. Now that we know more about what tools are out there, it's important to know both how and why to use them.

Larry Clinton is with the Internet Security Alliance, and he's going to speak a bit about why tools are needed, and what home and individual users should do.

MR. CLINTON: It's not a little television set. If there was one thing that I think I want consumers to understand about their home computer is that it's not a little TV. It's not a dumb, inanimate object that you sit down in front of and just drink stuff in.

Your home computer, particularly when connected to the Internet, is like your friend, your really, really, smart friend. Or maybe, better yet, your home computer connected to the Internet is like your very gifted child. You need to develop a relationship with it, you need to work with it, you need to communicate with it, you need to take care of it. And if you take care of it, it will take care of you. And you will learn wondrous things.

If you don't take care of it, you could have trouble -- a lot of it unanticipated -- and a lot of it very, very tough to deal with at later stages. So, what we are focused on for the moment here is not so much the technology as much as the behaviors that consumers need to adapt in order to become better computer citizens.

I'm going to deal with the first two parts of my presentation fairly quickly, who we are and why we

must take action, so I can spend, hopefully, more time on what it is we should do.

The Internet Security Alliance is a collaboration between the Electronic Industries Alliance, which is a 1,200 corporate member trade association, essentially, located over in Arlington, Virginia, and the CERT Coordination Center, at Carnegie Mellon University, which is pretty much the granddaddy of all the CERTs, and one of the experts, one of the leading experts, in vulnerability and threat analysis.

These are our corporate sponsors, these are the members of the board of directors. I point this out primarily to distance ourselves a little bit from most of what we're discussing today. The Internet Security Alliance is primarily focused not on individual consumers, we're really focused more on the corporate security level.

Last summer, we came out with this publication, "The Common Sense Guide for CEOs and Senior Managers for Internet Security." It's been pretty well reviewed. It was cited in the national strategy -- draft strategy -- TechNet has endorsed it, the U.S. council is now endorsing it, some overseas people are doing it.

After we came out with this, a number of people said, "Well, look. This is great. Why don't you come

out with something for the individual user?" And so we have, although frankly, it's not our main focus.

I think the primary benefit that I can offer today is not so much the content of what I'm about to say, but to simply provide consumers with a place to go where we have organized this information. So, we have one of these guides specifically for consumers and end users located on our website, isalliance.org.

Why we need to act? I think most of us in this room are pretty well familiar with this. This is a picture of the Internet as it was originally conceived, or thought of back in 1980. And at the time, this was thought to be very, very complex. This is the Internet now, graphically illustrated.

And by the way, it's kind of interesting. If you look at this, you notice that really intense kind of purplish area right there? I'm pretty sure that's the FTC.

(Laughter.)

MR. CLINTON: Here are some of the threats and attackers. Again, we have already gone over a number of these. The human agents are one of the things we're most concentrated about -- hackers, disgruntled employees, white collar criminals.

And I agree with the previous speaker, they're

going to get smarter, they're going to be involved with organized crime. Terrorists have received a lot of attention, and perhaps the fact that they may couple a physical attack with a subsequent cyber attack, which could be very threatening.

All of us on 9-11, I'm going to bet, did pretty much the same thing, which is we reached for an information system. We grabbed the telephone, we turned on the TV, we got on the Internet, and we were able to be reassured by the fact that we were able to see what was going on.

Imagine if the information systems were attacked and they went down, and we didn't know if there was a simultaneous attack going on in Florida or California, or if there was a chemical attack coupled with a physical attack. So that's very important on the terrorist level.

The one thing that we don't have on this that a number of people pointed out to me is we probably need to add another bullet, which is for pimply teenage kids in their basement. Very threatening human agent. Twenty-five of all the Internet attacks happen on Saturday night. One of the solutions we are looking into at the Internet Security Alliance is developing a website, GetaNerdaDate.com.

(Laughter.)

MR. CLINTON: We figure if we can get a lot of these kids out of their basement on Saturday night, we can do an awful lot to help with the Internet situation.

This is just the number of incidents reported to the CERT/CC. The actual numbers are not particularly interesting. What's interesting is the trend line, and actually, these numbers are vastly, vastly under-reported. Internet attacks are going way up, and here is the reason why.

As the sophistication of attacks is increasing, the amount of knowledge to create an attack is decreasing. So it's becoming easier and easier for all of us to use the Internet, it's becoming easier and easier for people to break into the Internet and cause us problems.

So, we finally get to what we should do. And this is the items that we have listed in the individual user common sense guide. I will go through them fairly briefly. A number of them have already been touched on.

The first is to use an anti-virus program. If there is only one thing that a consumer can do, for financial reasons, or whatever, this is what we would recommend, number one. We think it's your single best defense. Obviously, there are many ways to infect your

program -- floppies, CDs, e-mail, et cetera. Some of these programs will check these things automatically. Sometimes you have to check to see -- or sometimes they will check simply for the signatures.

There are new devices, that contain heuristics that actually go beyond the known signatures. The problem with these is that they tend to slow down service. And this is the real test that we have to get past, is what is the trade-off between increased security and increased functionality?

One of our big problems, on the behavioral level, is people turn off their security devices. One of the reasons why the vendors don't want to put out really secure software is consumers don't want it. So how do we deal with that problem? It's a major problem.

Number two is to keep your system patched. When the system acts erratically, obviously you want to know why. Usually you can contact your vendor. Some vendors will notify you automatically if you ask them to. Again, one of the problems is sometimes the patches cause additional problems, and sometimes even the vendors aren't aware of these problems.

So again, we need to have an interactive system, we need to work with the vendors, you need to tell them what's going wrong with your computer.

Number three is to use care when reading e-mails and attachments. I think by this time we're all pretty familiar with getting physical junk mail, and there is no real problem with reading any of that. But we all know that you have to be very careful with what you respond to when you get things electronically. Obviously, you don't even open it unless you know what's going on.

And the single best test for this -- and this is why we call it the common sense guide -- is does the message make sense. I remember, and I think it was back in 1998, when the I Love You Virus came through, I was fortunate, because the first I Love You notice I got came from somebody I did know, and I knew for a fact she didn't love me.

(Laughter.)

MR. CLINTON: Make sure the stuff makes sense. Number four, install and use a firewall program -- I think this has already been talked about -- a firewall is kind of like your security guard. It tells the packets where they can go and what they can go.

Now, the real hard part of the firewall is that eventually, you, the consumer, have to figure out what are the rules for what information should go here and there. Again, you must learn your computer, you must

know your computer, you need to work with your computer in order to make it functional and secure.

Number five, make back-ups of important file folders. A lot of us have fireproof boxes in our houses where we install our wills or vital information, maybe some pictures of our kids, or whatever. You need to do the same thing.

I know most of us -- I know I did -- learned the message the hard way with my first computer. I was in my first office, I lost my file, and the system manager came to me and said, "Did you save it?" And I said, "No, I wasn't finished yet." You save as you're going along. How often do you have to do this? Pretty often, unfortunately.

Number six, use strong personal passwords. One of the things that, behaviorally, we find we still have major problems with, everybody has got a password, and a lot of people have them right where they can see them on their cubicle, so they remember their password, and anybody can come along and get it directly.

Good passwords are strong, which usually means longer. They are unique, so you don't use "welcome" for all the passwords. They have to be remembered. You shouldn't be writing them down. And they have to be changed fairly often.

Number seven, you use care when downloading and installing programs. A lot of us get CDs in the mail. "You don't know where that CD has been," you tell your smart little gifted child computer, so you don't put it on there unless you are familiar with it. You have to consider the cost benefits.

Number eight, install a hardware firewall that's very similar to what we have already discussed.

And number nine, use access controls and/or encryption. A lot of us who have had kids know that early on, you spell things so that the kids don't know what you're talking about. That's encryption. And later on, the kids learn how to spell, so you have to use other sorts of things. Pretty much the same thing with your computer.

Again, it's not a TV, it's like an organism. You have to deal with it, you have to grow with it. If you do, you can make it secure and functional.

MR. SILVER: Thanks, Larry.

(Applause.)

MR. SILVER: Before we go on I just want to say we're running a bit behind schedule, so I would ask other panelists to keep that in mind.

Well, we know what the tools are, we have identified some of the threats that are faced, and we

have learned how to use the tools against the threats. So, a remaining question is whether consumers are actually putting these tools to work.

And I wanted to direct this question first to Anson Lee, of Symantec.

MR. LEE: In regards to the tools, yes, they are readily available. And we have talked about them: AV, anti-virus, firewalls, spyware detector, and the like. But unfortunately, most users aren't aware of these tools, because they aren't aware of the dangers that there currently are when they go on the Internet.

Most users don't really care about how the Internet works, or even how their computer works. They just want to know that they can get on the Internet when they turn on their computer and they log into their accounts.

What we have to do is to make them aware of these dangers, of viruses, of privacy threats, of hackers, and the like, that these things are constantly out there where we have individuals with programs and with these automated tools trying to find open systems to get into.

It's not exactly that they're out there looking specifically for Anson Lee's computer to break into, they're just looking for the first vulnerable target that

they can get into. And then when they're in, they can use those resources, whether it be the computer's hard drive, their high speed Internet access, or maybe whatever private or personal information is on that computer.

MR. SILVER: What usually leads consumers to purchase tools?

MR. LEE: Well, for anti-virus, it has usually been that they got infected, and they lost some data, and now they have to recreate that data. And now they have that experience of having been infected. They go out and purchase an AV product.

With firewalls and the like, it's usually because they are now hearing about Internet security threats, that they are adopting high-speed Internet access, and their ISP is probably telling them, "Oh, by the way, your computer is now on 24 hours a day, 7 days a week. If you leave your computer on, and your Internet connection is on all the time, you should think about a firewall."

But then users are thinking, "Gosh, that's a lot of work." A firewall typically is not an install-it-and-forget-about-it kind of program, whereas anti-virus is. You install it and you can forget about it. A firewall takes a bit of training for it to understand

what you're trying to do, what programs you want to allow to access the Internet, what types of activities you do on the Internet.

So it takes a fair amount of training. And for users, that's kind of inconvenient to them. They don't want to go ahead and train this program to be able to recognize, okay, this application or this program can access the Internet, while this other program cannot access the Internet. But again, it's all a matter of making users aware of the dangers of potentially what could happen.

And users also have this feeling of "Gosh, I'm just a home user, who is going to come into my computer? What's on my computer that's of value to anyone?" But for most of us here, we probably -- if we look in our computer, we've got a copy of our resume, more than likely we're doing our online banking, we're doing our online shopping, and what not.

These are all very important types of information, that if someone were to be able to get their hands on, it's prime to leading to identity theft.

MR. SILVER: Thanks. Software vendors are one source of information security tools, but PC vendors can also play a role in this area. Rich Lloyd is here from Dell to discuss some of their initiatives in this area.

MR. LLOYD: Yes, it's been a great panel so far. And certainly at Dell, we're excited about what we feel can be a pretty important role, as a PC vendor directly to the customer.

Before I get into what we're doing, I would be remiss if I didn't thank Larry for the new marketing concept. The PC as a gifted child. I think that will do very well.

In terms of what a hardware vendor can do, I think for a long time we saw ourselves as more of a facilitator. So we would be an early adopter of P3P. We would be a company that made Symantec and McAfee software readily available, provide custom-installed trial versions of the software, with the hope to snag customers and drive up the adoption rates.

I think we felt a responsibility to make as many of those commercially available tools available as possible. And for the most part, we sort of patted ourselves on the back as we were doing about as much as we could there. And then, of course, the data came back. And four percent of our customers told us they actually changed their P3P settings. Four percent. And about eight percent of customers actually took the McAfee 90-day trial and turned it into a purchased subscription.

We started thinking, is there a more proactive

role we can play? Because I believe the panel this morning was absolutely spot on. It has to be easy, it has to be transparent, and it has to be relatively costless. Because I would submit to you that the cost benefit analysis for an individual consumer around privacy is really somewhere in the $20 to $30 range, honestly.

And so, as a corporation, I have a fiduciary responsible to not break my commitments to Wall Street, and yet provide that kind of a value proposition. That's very difficult to do.

So, what are we doing? We believe we have got to change the paradigm a little bit at Dell. And we have got to make security and privacy really transparent on the box, itself. So, one of the things you will see us announce here in the next few days is factory-ready, installed Center for Internet Security benchmark configurations on the PCs, themselves.

And what does that mean? That means there is a level one benchmark, which Alan Paller will talk more about, factory installed on the system, that provides a little bit higher level of security and privacy on the machine without breaking things, that provides benchmark configurations for your OS settings that close off ports and do some other things that add just a little bit more

security than our traditional custom factory installs.

What we plan to do at Dell is to provide commercial offerings for folks that want to move up the grade, the security grade, and also move that out into other parts of our product set. I really believe that while demand for this kind of a product doesn't seem to be really strong in the consumer space right now, if we can make it transparent, if we can do it in a way that covers our fixed cost, and we can offer it on a variable cost basis, almost free or free, I really believe that you will see the demand -- which, right now, is fairly isolated to the public space -- move down into the consumer space.

And we're very, very excited about this thing. We have got to, as technology companies that have direct relationships with customers like we do at Dell, own up to the responsibility of making technology transparent. Because, unfortunately, despite all the good efforts of the W3C, of other groups that have done a really good job, in my opinion, putting publicly available technology in place, customers are not willing to invest, as was said earlier, the time, the money, and the effort to go about it.

So you have got to put it on the products they buy, and you have got to figure out a way to do it in a

way that makes economic sense for the market. And really, that's kind of the philosophy we're driving at Dell.

MR. SILVER: Thanks, Rich. Many of us shop online, and we may worry about our credit cards from time to time. Some companies are responding with tools to reduce the danger of using your card while shopping online. Mike MacCarthy, from Visa, will describe Visa's work in this area.

MR. MACCARTHY: Thanks, Jim. I want to talk about the Verified by Visa program, which many of you might have seen commercials about on television, but I want to give you some background about why we're doing it, what it is, and how it's working.

The Internet is the growing source of commerce for a lot of people, it's very important for our company. It's gone mainstream. More than 70 percent of all Americans are online these days. For Visa, it constitutes about six percent of all our retail sales. That's up from four percent last year, in 2001, and up from two percent in the year 2000. So this is a growing source of volume for Visa.

The channel is important to us for competitive reasons. We have 12 percent of all personal consumption expenditures generally, but we have well over 50 percent

of the retail sales on the Internet. So, electronic commerce is important for us to promote.

What is one of the major concerns that people have about shopping online? Survey after survey shows its concerns about security. "Surveying the Digital Future," a UCLA Internet report in February of this year, showed that 92 percent of all consumers are concerned about online security, 63 percent of them are very concerned.

According to research by a company called Payment One, released just last week, when consumers who have not made online purchases were asked what would persuade them to purchase more online, 53 percent of them cited more secure payment options. Payment security was chosen over price or product-related responses by a more than 2-to-1 margin.

So, there are major concerns about security online, so we thought we would step up to that concern, and focus on online security. Some internal data from Visa indicate the extent to which, from our internal perspective, security is important.

According to one of our Visa databases, in the third quarter of 2002, electronic commerce accounted for about 6 or 7 percent of all our sales, but it accounted for 15 percent of our fraud losses, and 23 percent of all

our chargebacks. Now, that's by dollar volume for those who keep track of that kind of stuff.

More figures that indicate the extent of the problem, in face-to-face transactions, only $.09 out of every $100 in sales was subject to a chargeback. That's for all of our volume.

For mail order, telephone order, it was $.27, and for electronic commerce, it's $.50 for every $100 was charged back. If we look at that from a transaction point of view, the trend is the same, 2 out of every 10,000 face-to-face transactions are charged back. For mail order, telephone order, the chargeback rate was 27 out of 10,000, and for electronic commerce it was up to 33 out of 10,000.

In the chargeback area, 71 percent of the electronic commerce disputes are cardholders alleging that they didn't do it at all. It wasn't that they didn't get the product that they ordered, or it wasn't what they wanted, it's, "We didn't do it at all." So 71 percent of our chargebacks are people who claim that it was someone else using the card, or they didn't do it, or whatever.

So, it's important, for our point of view, to have an electronic authentication or verification system. We think it will motivate a lot of non-shoppers to become

involved. It will reduce the chargeback and dispute numbers that we have got.

How does the system work? The way it starts initially is on the consumer side. Consumers have to sign up for the program. They can do it in a number of ways. When they open an account with a card issuer, they can sign up for Verified by Visa, and get their PIN number at that point. They can do it by going online to the issuing bank, and there is a process they can go through where they provide certain identifying numbers and information and get their PIN number at that point.

There is even a mechanism for doing it while they're shopping online. When they come to a merchant's website that is using Verified by Visa, some of the merchants have chosen to try to motivate using Verified by Visa by activating the Verified by Visa service at the point of sale. So, that's the first step. The card holder has to be involved in the process; it's his choice.

The merchant has to be involved in the process. They have to install software on their system, and the software has to meet the configurations and the standards set up by Visa to work.

But once that is done -- the cardholder has the PIN, and the software is installed on the merchant's site

-- it works in a reasonably transparent way for users. They go through the normal process of making a purchase online. And when they're about to actually make the payment, they then enter their account number.

At that point, a pop-up box appears, and they are asked to enter their PIN number. There is also a message that they previously recorded that says something like, "Hello, this is really Verified by Visa." It's a security feature that is put in there. But that pop-up box really is the opening of a communications channel between the cardholder and the cardholder's bank, the issuing bank.

The PIN number is inserted, there is a comparison between the PIN number and the account number. If they match, a notice is sent to the merchant that there is a match, that the person has been verified, and then the transaction goes forward as normal.

It's important to notice that the -- and as part of that transaction, the PIN number is not transmitted to the merchant. The PIN number goes to the issuing bank, it does not go to the merchant. You can't have fraudulent merchants setting things up and collecting PIN numbers.

How is it working? So far, we have to get a sufficient number of merchants signed up and a sufficient

number of card holders signed up so it makes sense for everybody. The Verified by Visa system is already up and working within the U.S.A. Visa-net. It's also installed and working internationally. All of the major processors of Visa systems are involved, and ready to work with it.

Nearly all of the U.S. issuers have implemented the Verified by Visa, or will do so in this year, and new merchants are coming on board and participating. The list of people -- we have Dell, who is one of our early adopters of the system. We have Disney, we have CompUSA, we have Orbit. Playstation.com is on board, Travelocity, JetBlue, more and more of the merchants are beginning to use the process.

It is a chicken and egg situation, where you have to motivate merchants to want to do it, and you have to motivate card holders to want to do it. It has to happen more or less simultaneously for the system to actually function.

For Visa, we have a lot of stakeholders in our system, and all of them have to get something out of a new product or service, otherwise it doesn't happen. For card holders, the advantages are straightforward. It authenticates their identity, it increases their confidence in shopping online, and it reduces the risk of unauthorized use of their card.

For the merchant, they get more consumer shopping protection against fraudulent use, and reduced dispute and chargeback incidents. For the issuers, for the banks that work with the card holders, they are comfortable that they are able to identify the card holder in these circumstances. They get increased sales volume, they get reduced fraud and dispute expenses.

The merchant banks, the acquiring banks in our system, they increase their sales volume, they have lower operational costs. All these disputes cost them money, too -- and this goes for new merchants in their system, as well. It's easier for them to acquire merchants.

So we think it's a product that has got some advantages. We think it's one of the tools that consumers will increasingly use on the Internet to protect themselves and to protect the information that they provide to merchants while they're shopping online.

MR. SILVER: Thanks, Mark. Let's discuss one final specific technology before moving on to some more general questions.

Many of us probably used these in the subway this morning. They are in our cell phones, and we also use them to access our offices. I'm talking about smart cards, of course. And Michael Willett has some remarks about them.

MR. WILLETT: Fasten your seat belt. This is going to be a fast tutorial on smart cards in the context of identity management and also a few current events that relate to smart cards.

Smart card, we're all familiar with this form factor. There are a number of other form factors, the most prevalent form factor is, in fact, a SIM card that fits into a cell telephone, mostly in Europe, and is used to provide identity management and credentials in the cell phone context. But this is the one we're familiar with, it's a little portable computer. Highly portable, highly secure operating system, data processor, et cetera.

Various form factors, I mentioned the SIM card, the slim credit-card size card -- this can be in the form of either contact or contactless. In the contactless case, it's used for access to buildings. Wave it in front of the little RF signal, it picks up the passive chip in here and does a little compute with the chip and verifies your identity, and in through the building you go. Or there's Easy Pass down the highway. So, there are various form factors.

There is a lot of physical and logical security built into smart cards, and it's improving every day. The one point I want to make here is that, in fact, the

way it's being used largely in applications is for securing and carrying and making portable your credentials. That is, the sum total of all the credentials that profile you, that's your identity, and I can carry my identity, then, in a portable fashion on a smart card.

A lot of services are available for smart cards. As I say, there is a little computer in here; most of the cards now are moving up to 64 kilobytes of memory, and lots of compute power. I can do data storage, authentication. I can do what's called multi-factor authentication.

That is, I have PIN access to the card. I may have biometric access beyond that. I may have challenge-response protocols that are handled by the smart card, so I can combine multi-factor authentication to provide strong authentication.

Cryptography is performed, digital signatures. It's an e-wallet, I can carry money in electronic fashion, I can carry, as I say, my profile for my identity management support. In more sensitive environments, I can have a shared intelligence between the card and a smart card reader that can be smarter. And so, the combination of the two can create a trusted environment.

Lots of applications. After issuing the card, I can still create applications that are new and downloadable to the card. Lots of advantages. One I will focus on here is privacy. That is where I put the control of my identity, of my profile, in the hand of the user. And through multi-factor and strong authentication, I have strong controls over the issuance of that identity. And each application can be designed so that it only accesses the minimal information needed for that application out of my sum total profile.

We have combined physical and logical bridging here between the physical world and the logical world. In some smart cards, hybrid cards, I can have pictures, I can have holographic images that make it hard to duplicate, like changing the color of the money from green to some off-green thing that we're doing with $20 bills.

I can embed the public and private key pairs with a public key. Lots of other credentials can be stored. I can imprint my driver's license on the card. There is a debate about whether driver's license should be a smart card or not. The American Association of DMVs is going through a harmonization exercise, and there is obvious resistance to using a smart card for a driver's license.

There are a number of hybrid uses. I could even put a mag stripe on here, and a holographic thing that could be read by optical readers.

Public key. Here is a very fast tutorial on public key. Alice creates two keys, F and G. F is public key, and that's published through a directory. G is kept private and secret. Bob wants to talk to Alice. Bob uses the public key to talk to Alice in coded messages, and Alice can be the only one that decrypts those messages using the private key. Alice, in theory, is the only one that converts ciphers back to messages.

Both those channels -- that is, the publication channel for public keys, and the cipher channel -- are available to eavesdroppers. So I can see, as a bad guy, both channels. My challenge then, which mathematics says I cannot do, is to recover the private key. I want to guess Alice's private key, knowing those two channels.

Now, the only thing missing here is that I want to make sure that Alice's public key, F, can't be spoofed by someone else imitating Alice. And so Alice does a registration process with a certificate authority, a well-known entity, trusted entity -- in some places, even the Post Office, in some countries, that is -- and the well-known entity, the certificate authority, certifies a copy of Alice's public key for distribution.

Two ways that smart cards enter into this picture. In confidentiality, for encryption, follow the bouncing ball here. Bob downloads the public key of Alice from the public directory. He encodes the session key that he wants to use with Alice, sends that to Alice. Alice uses her private key -- the only one that can do that -- to decode the session key, and then the two can use that shared session key over a public channel to do regular high-speed encryption.

So, the smart card, carrying Alice's private key, can do that deciphering step all in a trusted environment.

If I apply a public key in reverse order, that is, and let Bob apply his private key to a message digest that creates what's called a digital signature, Bob is the only one that can do that, in theory, because he's the only one in possession of the private key. Alice can retrieve the public key of Bob from the directory, and can decode, in a sense, the message digest, the signature, can convert it back into what it was originally, and compare to make sure that nothing in the message was altered.

So, by applying in an elegant fashion -- the private key first, then the public key -- we have a digital signature concept.

All of these things that I have described quickly here can be combined on a smart card. I can do the PKI, public key infrastructure stuff, I can store certificates, which are the certified copies of public keys, I can do the computation related to public and private keys, I can do the encryption, I can combine this with biometrics -- that is, I can use either facial geometry or fingerprint or iris scans, or handwriting dynamics, that sort of thing, I can store the minutiae for fingerprint, and do the local checking of identity, of biometric identity, locally on the card, as opposed to back at some central point.

Why have smart cards then, if they are so good, not been picked up in the United States as rapidly as in Europe? Even though we're coming on strong in the United States, as you will see by current events.

And I borrowed this chart. I have no idea why that person is doing that smoke thing in the corner. Must relate to this chart, somehow. Here are a few reasons why.

First, we have this neat little telecom system over which we have been exchanging credit card numbers for many years. Traditionally, until recently, we had very low fraud rates. But what you have already heard is that when we have card not present, or card holder not

present, these fraud rates go up dramatically.

No government-mandated card. I will say "yet," that's a personal observation. No government-owned telephone company. Should I say "yet?" And we don't have a health card, national health card system yet, either, in the United States. So those are some of the traditional differences between the Land of the Free and Europe that have, I think, impeded the growth of smart cards, but they're coming on strong.

Any of these market surveys, here is the latest one, it shows tremendous growth in all of the form factors, and all the dimensions for smart cards. And there is a good one you could -- I have given the website at the bottom, here -- it's a very good annual survey from Schlumberger, one of the smart card providers. They do an annual analysis of the marketplace, and I just extracted a few highlights from that.

SIM cards in mobile communication and telephones are still strong, but we are seeing the 64-kilobit cards coming on. Travel -- the contactless smart cards for access and travel are increasing by 25 percent. And JavaCard is getting to be the predominant operating environment for smart cards.

Going on this week is the largest, I think, and most attractive annual show in the United States for

smart cards, the Cardtech Securtech meeting going on in Orlando. That's why you have me. I think I'm the only guy in smart cards that couldn't afford the flight.

And here are some of the topics, some of the workshops that are going on there to show you what's being highlighted. Biometrics, anti-counterfeiting, contactless biometrics, and so on, and interoperability. Big issues.

The Department of Defense is now distributing what's called a CAC card, the common access card. It's to be ultimately used in all the military for personal identification -- that is, for storing your profile, access to buildings, and applications, encryption, digital signing, e-wallet functions, and medical data.

As I say, it's being distributed across the military now. Ultimately, 4 million cards will be distributed in the first wave. And there is a very simple -- this is nice about the issuance of such a large number of cards -- there is a very simple initialization issuance system based on two systems, called DEERS and RAPIDS, for distributing these cards.

At the same time, NIST is involved in promoting an interoperability function specification called the GSC-IS, the government smart card interoperability spec.

The problem, historically, is that applications

have been hard-welded to -- readers have been hard-welded to smart cards in a vertical proliferation of market. And so that's bad, right? Too many parts, and I want this part to run with that part.

So, the interoperability spec has introduced a grammar and some interfaces that will allow applications to uncouple from given smart cards, if you will. And so, NIST has been promoting that in not only the United States, but has gone on a grand tour here recently of Europe, trying to promote this spec.

The homeland security people are going to pick up on the CAC card, and are going to distribute it even further. There are some highlights about that. JavaCard, they're going to add memory. The current CAC card is 32 kilobytes, and they're going to add a little more memory, 64 kilobytes.

They're going to make a two-chip card, so that I will have a contactless card in there that allows building access in this version. So this is a big roll-out in the United States, based on the CAC card.

There is a group called the International Civil Aviation Organization, ICAO. They have just recommended, in Montreal, in fact, that facial recognition and contactless smart cards be combined so that I basically can put a smart card in a passport, I can smile into the

camera, and pass my passport near the reader, and the comparison can be made between my facial geometry and the stored image, just like you would be doing with a fingerprint. They like pictures of people better, because we're already having our picture taken, instead of being fingerprinted.

The United States, by the way, now coincidentally, is also requiring by October of next year that all foreign nationals entering the country will present travel documents with some form of biometric data. They also said they would endorse whatever the recommendations are of the ICAO.

So if you put transitivity together it tells you that the United States, by October of 2004, if all this time line falls in place, will require facial recognition contactless cards in passports. Just another form factor.

And finally, what's going on in Europe? In Belgium, they are rolling out a national identity card that will contain tax return information, change of address, civil records. It will provide access to all of those, it will contain some personal information, health care information, and so on.

Ultimately, the rollout is to 11 million citizens in Belgium. Same thing going on in Italy, so

we're seeing smart cards used in the identity management context.

In summary, what I would say is some of the strengths of smart cards in this identity management context are I have multi-factor authentication, mainly I have my profile, my personal information, in my control, especially given that applications are cryptographically portioned in this smart card to only access minimal information needed for a transaction. Thank you.

MR. SILVER: Thanks very much, Michael.

(Applause.)

MR. SILVER: Let's move now to some general discussion questions, and I want to pick Alan Paller's brain, first, with this question. Are the tools we have discussed so far sufficient to help consumers protect their information security?

MR. PALLER: Hardball, huh?

MR. SILVER: That's right.

MR. PALLER: Let's grade them a little bit on two criteria. One is are they transparent? I think Rich Lloyd's word is exactly the right word -- or Toby uses another term called "security baked in."

And we know, from panel one, that if they're not, they're pretty much irrelevant because if they're going to make everybody do a lot of work to use them,

nobody is going to use them. We have got hard data on that, and we know that's true. So that's A.

And B is do they do what the consumer thinks they do? Meaning, do they actually protect? So, I hate to do this to Mr. Smith, but his favorite kick-off was SSL, and SSL clearly wins on the first one, right? It's built into everything, we all know. But does it actually do what the consumer thinks it's doing? It gets an F on that.

Do you know why? Because although SSL protects your credit card information as it flows through the network, when it gets to the place where it's going, the company that put it there bought some out-of-the-box Microsoft web server and stuck all your credit card information on there, ready to be attacked, and no criminal is stupid enough to attack your home computer when he can collect millions of your credit cards from the vendors that do e-commerce with you. Which is why one of the things that Mark didn't talk about, but I think is one of the really big things that's a winner -- and I know we're going to talk about that in the other panel, I mean, in the other workshop -- is that they have a program that forces the merchants to encrypt the data.

If the merchant doesn't encrypt the data, you've got no sense in sending your credit card there.

Now, you don't care, because the merchants actually have to pay for the losses, but it's really a pain to have your credit card stolen, and have to go clean up after that. So you care enough that you don't want to do business with vendors that don't meet Visa's minimum requirements.

Second one we ought to give a grade to is the anti-virus tools. They get a very high grade on effectiveness, A-minus. The only reason they don't get a higher grade is that they miss all the new ones, right? I Love You got through because it got through before they had the profiles out. But they get a D or so on adoption, the Dell data gives you that data. They're just not being used, because they're not transparent, they're not built in, they're not baked in, so they're a wonderful tool if we used them, but we don't use them. So they don't get a high grade.

Even more so with firewalls. Firewalls are very effective, but they're not built in, and they're not transparent.

I think that the most useful thing that's happening here, in terms of tools that work, is something that actually Dick Clark was the godfather of, and Howard Schmidt did a lot of the follow-on work, which is the development of consensus standards. We're not going to

have government-mandated standards for security.

But they created something -- they helped create something back about two-and-a-half years ago, which was a gathering of federal agencies and big companies. Boeing, and Mrs. Fields Cookies, and Intel, and lots of companies got together to agree on what safe computing was. And because they did that, Dell was able to deliver out-of-the-box safe configurations.

And just to put that in perspective, do you remember Code Red, and how it infected lots and lots of people? Most of the people that it infected didn't know they had the software that was vulnerable, because the vendor had stuck that software in and turned it on without the buyer of the software knowing. And without consensus benchmarks, there is no way you can get users to configure the system safely.

So, I think the really high grade for this panel goes to Dell, even though it's the newest one, because they're doing security baked in that protects us.

The other grade that we will give is a Gentleman's C to Microsoft. They get As -- in fact, we're going to give them two of the security leadership awards in the summer -- for spectacular new things. But they get raw Fs in some other areas, and I just want to mention a couple of the raw Fs.

They have just come out with security benchmarks built into Windows 2003 server addition. But you can't buy an end user system with security benchmarks built in for Microsoft. You have to go to Dell to buy it, and you can't do that yet. But some time --

RICH LLOYD: Not ready quite yet, but we're getting close.

MR. PALLER: Some time shortly you will be able to do that. That's an F. Does that make sense? If they know enough to serve up the large companies, they ought to be doing it for the small -- for the other companies.

And the other one that Microsoft gets an A and an F for, is if you get XP, Windows XP, and you go through the installation script, they get an absolute A, because it asks you, "Do you want to have patches automatically delivered to your computer," and the default check is yes, as opposed to the default being no. The default check -- I know this is not okay to the privacy people, they want opt in. But this is one case where we like the opt out strategy.

So they give it to you, but they made a corporate decision not to do that for all the hundreds of millions of computers that are already out there. Now, I'm not looking for it on Windows 95, but Windows 98, Windows 2000, it's absolutely silly not to provide that

same kind of service, if only to charge us $10 a year, the way the anti-virus guys do.

MR. SILVER: Thanks, Alan. Let me pose a general question to anyone who wants to take it up, which is this. What incentives are needed, and also, which incentives already exist to develop new consumer tools for protection of information security?

MR. WILLETT: Well, if we just see what's happening in the web today, you will see the evolution, from browsing to information transfer, to what -- the big hot button these days is Web services.

And so, I think the incentive is there, by brute force. That is, we're going to be starting to see value transactions. That is, things that have real value, real monetary value, real intellectual value, exchanged more and more through Web services.

Standards are being developed in this area, the Oasis Standards Group, for example, is developing all sorts of interoperability languages using XML, and so all the ground work for Web services is being laid, I think, correctly. And so, Web services are going generate value transactions, a forced incentive for us to develop better privacy controls and better security controls in that environment.

At the same time, companies -- so many

companies -- are basing their life blood on their trust image, on their branding images. So I think there is a lot of incentive, from the business side, to be good citizens in the web services environment, because of the branding.

MR. MACCARTHY: And if I could just jump in, from Visa's point of view, the incentives are for us to promote good security practices on the Internet. I want to thank you for your kind comments about Visa's card holder information security, and for those of you who want to hear more about it, there is going to be another session on business tools, and the card holder information security program on June 4th. So, it's not the one that I will be talking about in this program.

But for that program, and for the Verified by Visa program, it's Visa's interest in promoting online commerce that is driving what we're doing. It has a good effect for consumers and for businesses, in promoting security online, but the motivation is, in part, promoting the brand, and in part, good corporate citizen. But in large part, it's promoting a channel of commerce in which we have a serious financial interest.

MR. SILVER: Larry Clinton?

MR. CLINTON: Yes, I would like to divide this into two different sections, one of which is what Mark

just spoke to, and Visa's a member of the alliance, and we're delighted to have them. They're one of our great examples.

We have some other corporations who are doing similar sorts of things. Nortel, for example, who is attempting to take their security needs and expand them out to their vendor community. And I think that profit motive is going to be the prime incentive in finding model instances such as Visa's -- to provide some sort of economic incentive for the current adult population.

And the business community, I think, is another thing, and I am joining Mark on the business panel, and we should go into that there, because I think there is a trickle-down effect.

But the second area that I think is really critical -- and I congratulate the FTC, and we have done a lot of work with Orson Swindle and Dan Caprio on this terrific stuff -- is the creation of the culture of security. And for that, what we need to do is talk about finding the incentives for our school systems to start teaching the sort of behaviors which will transcend the technological advances.

I mean, my daughter now comes home and is vehemently anti-smoking, vehemently anti-drug. I have an autistic son. But if I get in the car and don't put my

seat belt on, he screams at me, "You put your seat belt on now." Those of us who are my age know that, it used to be nobody would put a seat belt on. You know, a violation of our rights, and everybody smoked.

Not true anymore. We can change these cultures of security, but this is not being done, to my understanding, in the school system now. We are putting computers in all the schools, but we're not teaching kids cyber citizenship or cyber security. And I think that we need to have some sort of hand-in-glove situation so that when we have programs to get the school system connected to the Internet, which is a wonderful idea, and get computers in the schools, we also give them cyber citizenship, cyber security curriculum, because we need to grow this culture of security from the ground up.

MR. SILVER: Thanks. Richard?

MR. SMITH: Yes. I think the main incentive for the home user of getting better security in the products that they buy are actually incidences. I can just go down each one. If we look at Microsoft Word, it has better macro-virus protection in it, because that problem got out of hand.

We had Outlook Security Update come out after -- the first one after the Melissa Virus, and then we learned that wasn't good enough, and then the second one

was after the I Love You virus.

So, we have the CD universe case, which has driven more on the business side of protecting websites and information. That's all very reactive, and I think that's unfortunate. But it's going to be much better if we were more proactive about things.

I do think that Microsoft, being the primary vendor of software that we use in the home -- however, now, is being more proactive. We, unfortunately, have to wait two or three years for it.

I also share Alan's view that it's unfortunate that the older versions of Windows aren't being retrofitted with some of these same kind of security protections.

MR. SILVER: Thank you.

MR. PALLER: Can I throw something in?

MR. SILVER: Sure. Before you do, those of you with questions for the panel, if you would go ahead and line up at one of the mics, and we will take questions right after Alan Paller.

MR. PALLER: I love the idea of getting to the kids early. In fact, Governor Ridge and the Stay Safe Online Program at SANS annually has a poster contest for the kids, and they come to the White House, and they get prizes, and it's a wonderful idea.

It ain't going to change. It is absolutely essential, we must do it, but it isn't going to be even a bullet, a silver bullet. It's necessary, but absolutely insufficient.

I think a more important feature that earns another A for Microsoft in Windows 2003 -- it has the Nancy Reagan feature, the Just Say No feature. It has a feature that doesn't allow you to connect your computer to the server unless it has minimum anti-virus settings and firewall settings and other settings -- I don't know all the settings that are controllable.

But without that kind of technology built in, I don't think we're going to win just on the training, just the way we can't win safety in driving just by teaching kids safe driving. We also have to build safer cars. And it seems to me we need to build safer computers, and things like that Nancy Reagan feature help.

MR. SILVER: Thanks. Ari, were you first in line there?

MR. SCHWARTZ: Our part of the room is interested in -- and Ed Felten and Marty both raised similar questions to what I have, which were about smart cards. And Alan didn't give a grade to the smart cards, generally, and Rich didn't talk about building smart cards readers into the PCs.

It seems as though if it's going to catch on, it would be baked in, you're going to try security in that kind of way. I mean, obviously, there is still some security card work that still needs to be done on the smart card side. But in terms of the readers --

MR. WILLETT: Well, Dell is, of course, shipping -- there are a number of vendors that already sell card readers with integrated smart card readers in the keyboards, so that the whole keyboard becomes a trusted environment. And Dell is now shipping one of those as a base system.

MR. LLOYD: Yes I should have mentioned the smart card reader system, and I appreciate the reminder. We do see pretty good demand for the integrated smart card reader, although again, not the demand we would like shifting down into the consumer segment, which is the topic of discussion today. And the reasons for that have been well enumerated.

There is also a lot we are doing, from a middleware and a USB smart card reader perspective, in terms of bundling in the hardware. So, this is something that, like everything else, we're balancing the economic reality of demand for these things, but also trying to be at the forefront of the supply curve, putting these things out into the market.

MR. SILVER: And --

MR. WILLETT: You can actually have smart card readers integrated with keyboards with biometric readers on the keyboards. So the keyboard is getting to be a piece of intelligence, all by itself.

MR. SILVER: Next question?

PARTICIPANT: We want a grade, though.

MR. PALLER: You want a grade? You get a C, coming up for built-in, you get an A for effectiveness on one dimension, which is that it is the right way to keep people you don't want out of your systems. Having something that they have in their hand to get on the system, rather than a password, is absolutely essential.

All of us are moving to it. But it gets to the same problem as SSL, doesn't it, Ari, that at the other end, the credit card data is in an unencrypted database.

MR. LLOYD: And one thing I would just say, and you know, you hear this message from a company like ours a lot, but really, standards-based computing is what will help drive some of this stuff.

So, if you want to go back to the previous question, what are the incentives, well, the incentive -- to expose my private sector stripes even more -- the incentive is the creation of value. And the value gets created as standards are put in place, as Alan said, and

those standards make it easy and affordable for companies to provide widely accepted, widely standardized technology easily, cheaply to the masses, and then it gets adopted quickly.

And that's what we see with an example like Verified by Visa, where the creation of value is there. It's easy for a merchant to do it, because they make the money back in the shrinkage loss and in the chargeback loss. So it's a win for the company, it's a win for the consumer, and it's a win for Visa. That's the kind of program we have to have.

MR. PALLER: And they don't have to be government-mandated.

MR. LLOYD: No, it doesn't.

MR. PALLER: The Center for Internet Security showed, with Dick Clark and Howard Schmidt, that you can do it with a consortium of federal and consumer organizations and industry groups, and it doesn't have to be federally mandated.

MR. SILVER: Let's take another question. Does that mic work over there?

MS. BAUR: Yes. Hi, I'm Cynthia Baur, from the U.S. Department of Health and Human Services, and we actually have a national public health objective to increase Internet access in the home, and we're also

working on this concept of a national health information infrastructure.

So, from that perspective, I'm really interested in this idea of what consumers or patients or just people searching the Internet for health information, for example, could be expected to do and know.

And I would like to ground this conversation a little bit in the demographics of who we know has Internet access. And so, if we look at who is currently on the Internet, it's still higher education, higher income, and associated with that, is higher literacy. And along with literacy goes the ability not only to read, but to understand and do higher order thinking and understand things more abstractly and conceptually.

So, I am really interested in this idea of what it is that people can realistically be expected to understand and do, especially if I'm thinking about it from a public health perspective, and the flow of health information over the Internet.

So, I would just like to hear the panelists' comments on that, based in the demographics of Internet use.

MR. SILVER: Any takers?

MR. PALLER: Sure. Two threats. One is I will

get wrong information, and two is I will have bad things happen to me because I go somewhere where I shouldn't go. There are probably more threats, but let's just deal with those two.

If I am concerned about getting bad information, then we move into standards for -- just what Rich Lloyd was talking about -- standards for the websites I go to, and some testing method that I can be sure that they have their systems configured safely, according to some benchmarks.

And if we go to "I'm getting infected because I go there," that's solved by a re-engineering of the operating system. Microsoft has known how to do that for at least seven years, they have just consistently avoided doing the work that they need to do to make it possible for me to go to a website, and if the website is not known to be on the FTC's trusted list, then I don't allow that software to get into my operating system and screw me up.

I'm sure there are other threats that you want, but I don't think education is going to help if a person is worried about whether their kid is going to die of cancer. This whole idea of safe use of the Internet -- education just isn't going to be the solution.

MR. SILVER: Stephanie?

MS. PERRIN: Yes, Stephanie Perrin. I've got actually two questions, if I can. The first one is what do you think the impact of some of these privacy and security tools is going to be on trust in the consumers?

Example, I now run Microsoft XP -- sorry to pick on you guys again, Richard and Phil -- and I have configured my firewall to block everything going out, or at least alert me so I can make a choice.

Well, having worked at Zero-Knowledge Systems, it's not like I'm unaware of how buggy Microsoft's software is, but I am truly staggered at how often I get told that Microsoft is trying to talk to itself. And this makes me nervous.

And I am not a geek, definitely not a geek, but I am not a neophyte. So if I am nervous, what about the grand public out there. That's my first question.

And my second question is -- and it's similar to the SSL A and F problem that was brought up a minute ago -- with the smart cards. First you've got a problem that you really didn't address, how do you get beyond -- and I'm not suggesting you should have -- how do you get beyond the user acceptance, or the concept of an identity card. That's a big one.

But secondly, the threat scenario moves to the readers. How do I, as a user, know when it's safe to put

my card in a reader, because there will be people getting me to put my card in readers so they can run off, hack my card, get into the data, et cetera, et cetera. Right? Do we have any readers out there?

What kind of problems do we get into with wide scale deployment of smart card systems?

MR. WILLETT: Just a comment, and a mention of Microsoft there again, too. If you follow the Palladium initiative, and what's called TCG, Trusting Computing Group now, and TCPA, and all those other acronyms, in the whole industry there is a real shift toward moving trust and trustworthiness to the client side.

So there is a real focus in the industry on offloading the security from servers -- or at least balancing the security on servers with the client. So that's a general push.

And I think the other thing to do is just watch what happens in Belgium, or Italy, or one of these countries that's rolling out national ID cards with health information and so on, and they're having readers in the home, in kiosks, in public buildings, et cetera, massive deployment. It's just a matter of -- there is a practical environment in which the test limits, the system design of such a design.

But again, in technology, we are pushing toward

client trustworthiness, and we're rolling out systems today that should have the right safeguards built in.

MR. SMITH: Yes, I would like to address the firewall question. I think this has already come up. Firewalls are more -- of all the security products out there -- are one of the harder and more techy products to use.

And what you're pointing out here is, on one hand, you've got Microsoft XP phoning home to do an update, which is a good thing, and it's doing it a lot. So maybe there is a trust issue there. What is it really doing?

And a firewall really doesn't tell you that, it's just operating at a low level. So at some level, if you're going to use a firewall, it's going to require a higher level of training, I think, than some of these other products, unfortunately.

MR. WEITZNER: Thanks. I just have a question. I want to press any of you who are willing to be pressed on how we're really going to see more consumer individual user-level security -- and privacy, but I will -- we can leave privacy out of it for now.

And it's based on an observation that if you look at where security is actually developing, where there is actually progress, where Alan's grades average

above a C, as opposed to below a C, it does seem to be in what are basically centralized and large, but effectively closed networks.

So, I think, obviously, what Visa is doing is terrific. A lot of what banks are doing, the military is doing -- these are all centralized communities that are able to make top-down decisions about doing security, and able to push them, I think rightly, and say, "We're doing this now, guys, because we have a real problem."

And I look at the other side, the consumer side, and frankly, the Web side, including the Web services side, and these are decentralized networks where there ain't no one, including W3C, Oasis, or anyone else, who is able to say, "Okay, guys, we are doing it now."

As the gentleman from Dell said, certainly there are standards developing at W3C. We have a lot of the foundational XML security standards. Those are gradually being picked up into Web services, but I would emphasize the word "gradual."

And I just wonder what your thoughts are about whether -- well, I guess I want to express a note of skepticism about whether it's enough to say the market will sort it out for these consumer-level services. I believe that's the case when Visa has its network to worry about. I believe that's the case when the military

has its network to worry about. What about the rest of us, is the question.

MR. CLINTON: I appreciate the question, Danny, and I think the answer lies in segmentation. You know, there is a certain segment -- the early adopters, the current users, the people who are not geeks but know all about how to use a firewall and don't think they would be classified by the general population as geeks, with all due apologies.

I'm not so worried about them. They're going to read stuff, they're going to get on the Net, they're going to investigate, they're going to adopt the best available technology. They can afford it.

And then there is -- if I may go back to my education pitch. Stay Safe Online and a picture program at the White House are not what I'm talking about.

I'm talking about if you want to adopt a culture of security that is going to be part of the entire population, we've got to get them young, and I'm talking about curriculum taught in the schools. I'm talking about reading, writing, and computer skills and ethics as part of our general curriculum. That's where we're going to get this. Because the technology is going to continue to change. Now, those are the two extremes.

There is a big segment in the middle, which is

kind of us in the room, that I think is the more difficult segment. And I think, for them, you're going to need a whole variety of things. I agree that most of what we're talking about are the closed systems, and that's pretty much what I deal with at the security alliance.

I guess our best hope for this is the trickle-down effect, that we are going to be able to have good education programs -- and again, going to the next workshop session -- one of the things we're going to be talking about is incentives for businesses, and one of the things that we're finding out is that the most cost effective of all the security interventions that we're finding in the business community is training programs.

And we are hoping that when we train people in the Visa corporate network, they're going to go home and be individual consumers at home, and they're going to say to their husbands or wives, "Don't do that," "Don't download that."

So, we're going to have to have a messier way to get to that middle segment, and I don't hold out immediate hope. I don't think there is a silver technology, or a silver bullet anywhere. But that's the segment that's going to be tough to get, and I'm not sure we're going to get all the way there.

MR. SILVER: The last word goes to Anson Lee.

MR. LEE: Yes, definitely awareness and education is a key to this. And the government has a definite role to play. Because when we, as individual corporations, try to expound upon Internet security, they look at Symantec and say, "Oh, they're just trying to sell product." But when you have the government saying, "Well, this is what it takes to be secure, or to be a good citizen on the Internet, and these are the steps that you can take, go ahead and take a look at the tools that are out there and go ahead and make your own decision," because when you know what is actually going on you can make a better informed choice of what is right for you, as you are sitting at home in front of your computer, doing what it is you want to do on the computer.

MR. SILVER: Well, we have consumed 10 minutes of lunch time. But please come back at 1:00 for panel 3, and I want to thank this panel for a very informative discussion.

(Applause.)

(Whereupon, at 12:11 p.m., a luncheon recess was taken.)

A F T E R N O O N S E S S I O N

INTRODUCTORY REMARKS FOR AFTERNOON PANELS

MS. LEVIN: If everyone would please take their seats, we would like to get started.

MS. GARRISON: Good afternoon, everyone. I hope you all had a nice lunch break. Welcome to the third panel for the Federal Trade Commission's public workshop on technologies for protecting personal information.

I am Loretta Garrison, and I am going to be your moderator for this afternoon's opening session. But first, to open the afternoon discussion, it's my pleasure to introduce to you all Commissioner Mozelle Thompson. Commissioner?

(Applause.)

COMMISSIONER THOMPSON: Good afternoon. First of all, you guys can move in closer, you know. This isn't a continuation of the spam workshop.

Well, it's good to see you all here. I see a lot of familiar faces from the work that we have done here in the areas of online privacy and security. And you're still standing, so this is good. You should give yourselves a hand, this is a good thing.

I want to just take a second to talk about what the workshops that we're having today and what follows,

what it's about and what it's not about.

It's a really easy tendency in today's climate of talking about terrorism and other subjects, that when we talk about personal information, to focus solely on security. And there are others who would want to focus solely on privacy. But the reality is that both coexist, and in many cases, they coincide.

But they are very different things, and I think we will explore that a little in the context of our discussions. And along with additional consumer protections like protections against fraud and deception, we have a bundle of tools that consumers need to focus on in order to feel comfortable about participating in the online environment.

Because it's no secret that the current economic conditions and the world of high tech have resulted in a more demand-driven marketplace, one where businesses and governments alike are focusing on how do we retain consumers' interests and build their confidence?

Now, this morning, we heard about some of the tools available to help consumers manage the collection and use of their personal information, as well as some of the tools available to help them manage the security of that information.

As some of the panelists were quick to point out, some of those tools have been successful, and some of them have not been quite as successful. So, we have begun to scope out what some of the limits of technology might be, as well, at least in our current state.

So, it's appropriate today that we are having discussions about the consumer perspective in considering technologies for protecting personal information. Because the consumer's use of the Internet has not reached its potential yet, but we all have great visions of a vibrant and strong global marketplace.

But that only happens if consumers feel that they're the center of the value proposition. In other words, that the market recognizes their importance, and is able to pay attention to and cater to what consumers feel they need to be safe and confident.

Now, among those tools are rights and remedies that can protect them from harm, like fraud and deception and security breaches, and privacy violations. And I think that we at the FTC know something about that.

But we also have a role in incentivizing technological responses, and talking about what all of us at the table -- that's government and business and consumers alike -- can do together to help manage this problem.

Now, it begins by all of us not operating in a vacuum, being able to listen, solicit, and understand the consumer perspective so that we can talk about what are realistic expectations, and what are not, from technology.

We also need to understand better consumer behavior, what drives them to make choices, and what they think they understand about the online world. Those will help to inform our policy decisions.

So, today, and this afternoon, we begin with a distinguished panel, who will begin talking about consumer behavior, including issues dealing with trust.

And later this afternoon, we will talk about what's been done in the area of identity management systems, and consumer issues raised by those technologies.

So, now, I encourage you to participate as actively as possible. Those who do not will not get cookies at the break. The fact is that the people who are here have been engaged for a long time and serve a very important role at helping to chart a course for what we do next, what does the future look like. And I think you should all feel good about that.

So, I am interested in hearing what our panelists have to say, including what we should be doing

and maybe some of the things we shouldn't be doing. And so welcome, and let's get started.

MS. GARRISON: Thank you, Commission Thompson.

(Applause.)

1

PANEL 3: MAKING EFFECTIVE USE OF TECHNOLOGY: UNDERSTANDING CONSUMER BEHAVIOR

MS. GARRISON: As the Commissioner said, this panel is going to explore the dimensions of human behavior and interactions with technology. I am certain that this discussion will resonate with everyone in this room who, no doubt, has, at one time or other, been challenged by new technology or tools or toys that affect our lives daily.

This panel is going to have two parts to it. First, we will hear presentations by three distinguished academics who are here to share their work on understanding human behavior. At the conclusion of their presentations, these three panelists will be joined by people who work with consumers in a variety of contexts, and who know, first hand, the problems that many consumers have in dealing with technology.

Our three presenters, seated to my right at the far end, are first, Andrew Patrick, who is a senior scientist of the Network Computing Group, Institute for Information Technology, National Research Council of Canada.

Next is Donna Hoffman, professor and co-director of the Sloan Center for Internet Retailing, the Owen Graduate School of Management at Vanderbilt

University.

And next is Mary Culnan, Slade Professor of Management and Information Technology, from Bentley College. Also joining me is Toby Levin, who will be assisting with this afternoon's presentation.

Andrew is going to open our discussion with a discussion on human factors of privacy-protecting systems, and how to incorporate such factors into system design. We know that people handle technology in many different ways. Some adapt comfortably, while others constantly struggle. Andrew will provide insight into how technology should be designed so that people can easily use it. Andrew?

MR. PATRICK: Great, thank you. First of all, I should come clean. I am a psychologist, but I have to admit I am also a geek. I do know how to run a firewall, both a hardware firewall and a software firewall. And like just about everyone else, I do run a home network and do have three teenagers who are using the network. But I do live and breathe the problems, as well.

Yesterday we were victim to a drive-by download, which is a download that comes when you visit a website, and it installed some spyware that was deciding what advertisements I was going to see.

What I want to talk today is to introduce some

ideas about thinking about consumers from a psychology point of view, and that is getting into their heads, and taking into account what we know about how people think, how they make decisions, and what their features are, and what their limitations are, if you will, and what that can tell us for privacy protection and building usable security.

Let me begin by giving you just some numbers. These numbers come from a study reported in 2002 at the human factors conference, looking at users' concerns about privacy and security. And what they found in doing detailed interviews was that just about everybody was concerned. They were concerned about risks or harms going on the Internet.

And just about everybody felt that something should be done about it. They didn't quite know what, but something should be done about it.

The areas that were of most concern fall into three categories: information security, which is, as we have heard, does the information that is being passed around the Internet, is it getting to the right place, and is it getting there securely; and also information privacy, what's happening to my information once it does arrive, how is it being used, and so on.

The second category of concern was concern for

the users of the Internet. What are you going to experience? Am I going to experience something that I am not comfortable with? And what about my children? Are my children going to experience something that I am not comfortable with?

And the third category is what's going to happen to my system? I just bought this shiny new system and brought it home, and got it connected to the Internet. What's going to happen to that? Are there threats to my computer? Is it going to get hacked, get broken in some way?

Those were the areas of concern, and I'm going to focus mostly on privacy. The research that I have been doing is really looking at users' concerns, and ways we can mediate those concerns in the area of privacy.

We have been working on a project which I like to call usable privacy, which is really taking a human factors approach, combining what we know about people and what we know about technology to try and build better systems. We have been doing this in the context of the privacy regime in Europe, because we're working with European partners, and in Canada, where I'm from.

As we heard this morning, some of the drivers are stronger in Europe and in Canada, because of the legislative environment than they are in other places.

And so it's provided a nice context for working in the area of privacy. But we are also looking at generalizing to other regimes, as well.

So, we have been emphasizing the European privacy directive, both the EU directive and national directives, and also looking at privacy principles, those that come from other organizations, the OECD, et cetera, and really emphasizing something called usable compliance, which is if you have to comply with particular privacy principles, either because they are best practices or because they are mandated, how do you do so in a way that's actually going to be effective to your consumers? And what do the privacy principles really mean for human factors, and for good design?

You have probably already seen lists of privacy principles. This is a list that has been extracted out of the EU privacy directive. It's very similar to lists that have come from other organizations and from the OECD.

The most important principles are things like transparent processing. That is, processing the data in a way that is visible to the people affected by that data.

I should point out we have been using transparency in two different ways this morning. One is

transparency in the sense of being able to see the manipulation and operation on the data. So as my private information moves around, we are suggesting that it should be transparent, I should be able to go in and examine it, and hopefully be able to rectify any errors.

The other use of transparency is the exact opposite. When we talk about SSL, for example, people describe it as being great because it's transparent. You don't see it operate at all. And in that particular case, it's really transparency in the sense that its operation is transparent to the user. Everything is hidden.

I think we need to clarify this, and really try to come up with some better language. Both things are very important, in particular contexts.

What I want to do is teach you five new words -- or five old words -- to keep in mind for the rest of the afternoon, and hopefully, for the rest of your careers. They really have to do with what do we have to do to support usable privacy, usable security, usable systems in a way that people can actually use?

And so, one of the ways to think about it is what is the end user, the consumer, being asked to do?

So, the first thing they are being asked to do is comprehend, and we heard a lot about this this

morning. Users are being asked to understand a lot. They are being asked to understand how the systems work, but also privacy concepts, what the risks are, and so on.

The second thing that users are really being asked to do is be conscious of the right thing at the right time. So, not only do they have to be able to understand things, they also have to know when to draw on those memories, when to draw on that knowledge at the right time to make the right decision.

So, we can think about comprehension as kind of being in the back of the mind, the background knowledge that people have, their general understanding, whereas consciousness is what's in the front of their mind, what are they paying attention to?

So, when they are doing something related to privacy, we want to make sure that those things, their knowledge, is at the front of their mind, and they are making their decisions in the context of what they know.

The third concept is control. That is, we must build systems that people can actually use. We must build widgets and screen interfaces and buttons that people can actually control. If we have a system that allows people to control privacy preferences but they can't find it, they can't locate the buttons, they can't use the interface, then that causes a problem.

And the fourth thing on this slide is consent. In the privacy domain, there is a key concept of consent. Users must be able to make decisions and give active consent and revoke consent. And so, when we build our systems, we must make sure we support consent. So consent is really what people explicitly say. And this is a key concept in the European privacy legislation, for example.

So, in comprehension, for example, we heard a lot about what people are being asked to understand -- we talked about education already this morning, and training, and help systems, and pamphlets, the kinds of things that are being used.

So, the challenges really are how do we present the information, how much information do we present? What are the words and the phrases? We heard a lot about P3P and the issue of what kinds of phrasing we use to display concepts. And some of this stuff is really hard.

I understand from some of Lorrie's work that I think there is something like 36,000 possible combinations for P3P settings. The complexity is quite hard, so asking people to understand that is quite hard, let alone trying to understand simply what a cookie is and what it can be used for.

Consciousness, again, this is getting the right

thing in people's awareness at the right time. There are lots of human factors techniques that can be used here, things like pop-up windows, alarms, highlighting, sounds. There is quite a tradition here.

It's quite important -- again, drawing on some of Lorrie's work -- we know, for example, in privacy, people often aren't paying attention to the things that they probably should be paying attention to. So, for example, we know that reading privacy policies is pretty rare.

In control, control really has to do with if users understand that they need to do something, and they are aware that they need to do it, can they actually do it? Have we built an interface that they can actually use? So this has to do, really, with the principle of obviousness, or affordances. Is the interface such that finding the thing to do for controlling what you want to do, is it obvious enough that people can actually find it?

So, in terms of privacy control, for example, are the opt in and opt out controls easily located, and are they easily understood? One of the things that's interesting is people often have a great deal of difficulty explaining what their privacy preferences are, and they often change, depending on the context.

And so, people may say they have a general privacy preference, but in a particular context, they may be willing to modify that, depending on the kinds of service. And we have already heard a little bit about the importance of default settings, how getting people to change default settings can be difficult, and so choosing reasonable default settings can be quite important.

The last issue is consent. The principle of informed consent is quite important. The idea is that people are making decisions with the appropriate information to support that decision. And so, one of the ways we see consent right now is in user agreements.

So when you sign up for a service, or when you install software, you have likely seen a large legally worded agreement that says, "If you're going to use this software, you must click here after reading this very long agreement," and we know that most people don't do that. They don't read that agreement, they click anyway.

So, that really doesn't support this idea of usable compliance with privacy principles. We need something better than these big, long agreements. We need some way of supporting that.

One of the things we have been experimenting with -- because we know that people ignore user agreements -- is click-through agreements. We know that

asking for a general consent, particularly for a large service such as a portal, really isn't appropriate, because the consent may be quite different for different aspects of the service.

And we really want to be able to track specific things that people have agreed to, and things they haven't agreed to.

One of the concepts that we have been experimenting with in the lab is a concept of just-in-time click-through agreements, very similar to the short notices we heard about this morning, where agreements are broken down into components, and particular parts of the agreement are brought up in the context of which they're important.

The EU directive, for example, says that there is a certain class of information that is particularly sensitive, such as trade union membership. And so, the concept here is a test such that when people are asked to fill in a field for trade union membership, as soon as they click on that field a special pop-up agreement comes up, and it provides the context for what exactly they are agreeing to be processed here.

One of the problems we're finding in the lab in initial testing, by the way, is people have learned to ignore all pop-ups.

(Laughter.)

MR. PATRICK: All pop-ups are ads, and so we're getting some phenomena for some users, where they simply dismiss it very, very quickly, and we know they're not reading it. And they tell us that, "Oh, I just thought that was an advertisement." So we're looking at other methods to support the same thing.

So, last slide, five things to remember. Comprehension, consciousness, control, and consent, and the last one is context. I didn't talk a lot about context, but context is really important, which basically says all of these things that consumers do are done in a context, and that context changes.

So, my role in my office environment is different than my role at home and as a parent, and so I am likely going to have different privacy preferences, different security concerns, and therefore, I am going to need different kinds of set-up and different kinds of support in those two situations.

MS. GARRISON: Thank you very much, Andrew.

(Applause.)

MS. GARRISON: Next, Mary Culnan will examine consumer behavior regarding trust and technology from a social marketing perspective. Mary?

MS. CULNAN: Thanks, Loretta, and thanks to the

FTC for inviting me to be here. It's always nice to be back. I think we were here just about a year ago, talking about this.

But since we are at the FTC, and accuracy and non-deceptive communication is very important, I'm not exactly going to talk about what Loretta said I'm going to talk about, so you will just have to see.

My talk is going to reinforce some of the comments we heard in the second panel in the morning, and also I thought what was interesting when I saw Andrew's slides was how those of us that are working in different areas on this, we use different language and different concepts to explain basically the same phenomenon. So at least there is some convergence.

So, what is the problem? I want to talk about a slightly different problem than I have been hearing most of the morning, which is how consumers can protect their own personal information. And I want to talk about how, as a society, we need to protect ourselves from consumers and their unsecured computers, which is what we talked about last May.

And I think sometimes these things get mushed together, as the privacy topics get mushed together, and it's really important to sort things out. But I think it's not a secret that unprotected consumer broadband

connections are becoming a greater and greater threat to the country. They are a vulnerability because they could be launching pads for spam, for denial of service attacks, and who knows whatever.

So, the real issue here is that this is potentially a national security issue, and I think that's why it deserves to have a lot more importance than we're placing on it currently, and really try to solve it.

Okay. If you looked at the national strategy to secure cyber space that came out in February of 2002 -- which did not have particularly satisfying recommendations for this part of the problem but it's basically we can all help if we secure our home computers. That's pretty much a given.

And then it talks a little bit about what the Department of Homeland Security is going to do, in terms of education and awareness, a little bit of curriculum development, and then trying to bring some of the vendors to the table to try to help make things easier on the consumer side, when they get their systems and sign up for an Internet account.

The problem is -- we also heard this this morning, but I think it's important to reiterate this -- that education and awareness are not enough. You really need to change behavior. All the websites in the world

and software loaded on your machine are not going to change behavior. And as long as people don't really understand that this is a real problem for them, and that it could really happen to them -- and as we heard also -- then people tend to react.

And I think some of the stuff that's out there now, while it's a good start, and it's helpful, it's really the field of dreams because people aren't going to go and do it on their own if they don't even know it's a problem. So awareness doesn't always lead to action.

And particularly, I think installed software doesn't always get updated, and in my own family, I have seen that with my parents and then my two brothers. One brother is just now deciding he may need some virus software. I said, "Yes, this is a good idea, go get it." My other brother had virus software but never updated it, and his machine got taken over by a virus and had to go to the computer doctor, and et cetera, et cetera.

And then my parents, I just update theirs without saying anything when I go visit them, because I say, "Have you updated your virus software?" "Yes, we got new software last January." No, I don't think that's going to do it.

So, again, because of my interest in this, some colleagues at Bentley and I are starting a small research

project. And what I'm going to talk about today are not the results, but sort of the approach that we're taking to frame this issue, and hopefully come up with some ideas for how to tackle this from a social marketing perspective.

So, social marketing is really about taking what is used in the private sector to sell soup and soap and toothbrushes and everything else, taking these same techniques and applying them to social problems, where the basic idea is you want to change behavior. You don't just want to make people aware, but you want them to do something.

Examples of social marketing programs have included trying to get people to stop smoking, getting people to use seat belts. A lot of the public service ads we see on TV are aimed at that, but the ads are not enough.

And how it differs from commercial marketing is here you have marketing techniques being used to benefit society at large, not to benefit a particular single organization. And on the slide, there is a citation to a book by a professor at Georgetown who is probably one of the leading social marketing experts in the country. So if anybody wants to follow up on this, you can get in touch with him.

So, in marketing, there are what are called the four Ps, and these are product, price, place, promotion. Product -- what it is, whatever it is you're selling; the price that people are willing to pay for this; place -- how are you going to distribute the goods, get them in their hands; and then, promotion -- you have to make people aware that the product or service exists and that they want it.

And so, any effective campaign to get people to change their behavior related to security is going to need all four of these.

So the product -- we heard about this this morning on the second panel -- in terms of not just getting people to buy single products, but basically to create a culture of security in their own homes, on their own systems, and the list of what this includes is pretty standard.

And I took this from a NIST report. Since I'm not a security guru, I figured if it was good enough for NIST, it was good enough for me.

Okay. Pricing decisions. Here, people make their decisions. It's both on the cost and the benefits. And so, doing security, there are a certain number of hassle factors, which include the price -- not only of just acquiring the software, which is not a particularly

expensive thing, but sometimes it doesn't interoperate.

I have big problems with my own firewall, where it doesn't fire up automatically. Sometimes I can't get on to the Internet. It's just -- you have to be very dedicated to make this continue to work. And so I think that's important, to keep working on the technical side.

On the distribution side of things, the place that basically the behavior must be easy to do. And currently, I think too much of the burden is on the consumer, although we are starting to see some things that are improving. You do get anti-virus software on your computer, although we heard from the gentleman from Dell this morning that most people don't extend their complimentary subscription.

Window XP now comes with a firewall that I understand is turned on when you get your machine, which is an improvement from what we heard about last spring. And you get reminders to update your software. But again, people don't necessarily take the action.

Then there is some anecdotal evidence that the ISPs could do more than they are currently doing. And I think this is very important, since they're the ones that are actually the touch point with the consumer, when people get their broadband connections.

I know in my own case, when I got my cable

modem, the guy who was a contractor who installed it never said a word about a firewall. There was nothing in the box, nothing in the package they gave me that suggested I needed to do this. I knew I did, so I went out to the computer store, and was told, "You already have one."

But another example is a friend of mine who lives here in Washington and just got a cable modem. And again, nobody said anything to her about a firewall. I talked to her on the phone, and she said, "Oh, I installed a firewall," and I asked "Well, why did you do this?" I mean, this is a good thing to do.

And she said she had wanted to move her laptop around the house, and was told she couldn't do this because she only had one plug and she needed to get a router. Well, she didn't know what a router was, so she was surfing on the website for the ISP and stumbled across an offer to download a firewall, so she thought she would do that.

On the promotions side, we need more than just advertising and websites, and I think we have heard this already. This technique can include personal selling, and it includes some tactics that are basically going to reward consumers if they do the right thing. And what we need to do is figure out what these are and how to make

them work.

And finally, execution. And I think this is one of the issues is one size does not fit all, because all consumers are not the same. If you think about when you watch commercials on TV, I mean, a lot of times I know I'm not watching a show that I'm supposed to be watching, because the ads are nothing that I would be interested in, either because they're too young or too old. So, you know, there is targeting of messages.

And in fact, last year, when we talked about this, there was a lot of discussion about automobile analogies. And in the New York Times on Monday, there was an article that there is now going to be a new TV ad campaign for seat belts, focusing on high risk drivers. So this is a great example of developing a message and targeting it toward the appropriate segment.

Men in a particular age group don't use seat belts. They are not motivated by the "You are going to die in a big crash" message. What they found out is these people are motivated by what not wanting to get a ticket. And so they have developed some PSAs that they think will reach 70 percent of this population. The message is, "If you don't have your seat belt on, the cop will give you a ticket, you don't want a ticket, so use your seat belt." And they are going to show this on fear

factor, NASCAR racing, baseball games, okay?

(Laughter.)

MS. CULNAN: So if you don't watch this kind of stuff, you're not going to see these ads, but they expect this message, hopefully, will reach the right audience, and will have some effect. So we need to do segmentation, and need different strategies that are appropriate, based on the characteristics of the different segments to drive the change.

And then finally, we know a lot about what people say they believe about privacy, we know a lot about their attitudes. We don't really have anything comparable for security. So one of the things my colleagues and I are going to do in our study, once we have decided what we need to measure, we're going to do a public opinion survey related to security to get a sense of where people are, what they do, what they don't do, and try to get some beginning good data on that.

Again, the question is why don't the vendors do more? Is it cost? I thought what Dell announced this morning was terrific. Are the vendors concerned about liability? They don't want to answer the phone? I mean, even when you get through on the phone, basically you don't get good advice regarding firewalls -- at least I haven't, from my ISP.

Better usability. I remember talking to Richard Purcell about this when he was still at Microsoft. You get the announcement of the automatic update, and you think, "Why do I need this? It has nothing to do with anything I am doing." Maybe there could be some wizards or something that could help you sort out what you needed to install for your own particular user context and environment.

There are also trust issues, I think, with automatic updates. I have a colleague who works for the attorney general's office in Massachusetts, and he basically doesn't trust anybody coming in on his system because he doesn't know what they're doing.

And then education is really everybody's job. The government is talking about doing K to 12. We heard about that. You need to get kids while they're really young, that's really important. But there are a lot of other opportunities to do training for the rest of us. Employers were mentioned. I think that's a great place.

You know, if they're doing training on something, or even if they're not, they are the ones that are likely to have their systems attacked. So it's in the employers' interest to make sure that their employees are not the ones that are unknowingly going to cause this to happen.

In the universities, there is always a core information systems or information technology course in every college. It's not just for business school students; everybody pretty much has to take that.

When I first started teaching, the big issue was backing up your disks. I mean, we had undergraduate students who thought they could make it through four years of college with one five-and-a-quarter inch floppy disk. Things always got destroyed. So, part of the education was, spend another dollar, buy another disk, and this can make your life a lot better.

Well, the world has changed. We don't worry so much about floppy disks any more, but this is a really good place to teach these people security, because they are interested. They don't want their systems to be taken over.

In my own case, I had one student who actually said, "Well, I know our systems are protected here, because we're running on a network. But I don't have any idea. What am I supposed to do after I graduate?" And I thought that was exactly the right question to ask.

MS. GARRISON: Thank you very much, Mary.

(Applause.)

MS. GARRISON: And finally, Donna Hoffman will

discuss some preliminary research on privacy, security, and trust issues, and look at factors that make consumers more willing to share their information when making online purchases.

MS. HOFFMAN: Thank you very much, Loretta. I am very glad to be here today, and I want to thank the FTC for inviting me. I am also especially delighted to be able to take a break from the tornadoes and the flash floods that I have been experiencing a little bit too close for comfort, I must say in my own case, since we had a flash flood in our back yard. And so I am really enjoying the gorgeous weather here today, and hoping we won't get some rain for a while.

Now, my objective here today in the short time that I have is just to introduce some ideas to you and hope to set this up as a platform for discussion. I also want to give you an early look at where we're going to be going with some of our own research in this area.

So, I want to say a few words about marketer/consumer tensions, lead into some thoughts that I have had about the privacy paradox, and then I want to very briefly review some recent research which has really got us thinking about a number of issues in this area, with respect to consumer behavior, and then talk a little bit about a research agenda going forward.

And one thing I should say is since I tend to come from the Evelyn Woods School of presentations, there is a handout of my presentation in your pack, and you might want to look at that as I go.

I am skipping over some of the slides. I have put some references at the end and there is a URL, so if you want to download the presentation, it's available on the e-lab website as well, and I know it's also on the FTC site. So that's just some fair warning that I'm not going to necessarily talk about everything that's on all the slides.

One of the things that I think is particularly interesting is that online marketers, as we know, want a lot of detailed information about consumers so that they can segment them into groups, for example, for purposes of target marketing efforts, and for personalized offerings.

Now, research shows pretty clearly that consumers actually appear to appreciate these personalization efforts if it seems to suit their needs. Now, at the same time, consumers report that they are very wary about just what are they collecting about me, how are they using it, for what purposes are they using it. A lot of this is arising because of what we could term bad behavior by marketers.

And one of the things that we have come to realize is that spam is contributing enormously to this problem, particularly in the recent past, because consumers ask, "God, how did they get my e-mail address? Where is this stuff coming from?" And so that contributes to this perception, and it's increasing these tensions and conflicts between online marketers and consumers.

And so, while the consumers do want this personalization, and are using these services, they like the idea that the sites are collecting this information, and they are willing to give out this personal or private data in order to get this experience.

But at the same time, consumers are very concerned about their privacy, and they are beginning to wonder what's happening to this information. And it's pretty clear that they want a greater degree of control over how this information is used. And if you talk to them, what they will tell you is, "I would really like some sort of guarantee," whatever that means, "that the data will not be misused."

Now, a lot of this is arising because of things like, for example, cookies and capturing click stream data, and web bugs, which marketers use and which don't require consent. A lot of increase in offline and online

data aggregation and cross-site data sharing. There might be some consent on the part of consumers, but consumers don't really have a very good expectation about what's happening with that data.

And one thing that is very clear is they have an expectation that those kind of data will not be sold. And of course, in many cases, they are sold. And in some cases, there is no consent at all.

So, a lot of these explicit and implicit data collection efforts through personalization, for example, or through digital downloads, are really creating a lot of wariness on the part of consumers.

And so, one of the things that becomes very clear is that control emerges from a lot of this research as the key issue. And regardless of what survey you look at, you can see that these are the top concerns.

Now, I haven't ranked them, because it depends on what survey. But consumers are very concerned about the third-party data issue -- who has access, what's been collected, how is my data being used, who is getting a look at it, my data are not secure, and then this idea about hackers and identity theft.

And so, it's really no surprise that there is a lot happening in this area, and that consumers are becoming increasingly wary and concerned.

Now, that leads to this idea of the privacy paradox. And basically, that's this notion that consumers' own attitudes and behaviors themselves seem to be in conflict. So we don't just have this consumer/marketer tension, but we also have these consumers in tension with themselves.

And what that comes from is the idea that surveys consistently show that consumers are very concerned about information privacy. Yet, at the same time, they continue to provide their personal information.

One way to think about this is what's up with that? And if you start to really think about it, what you can see is that they are not really in conflict, we're just looking at things from different perspectives.

If you look at the attitudinal studies, what you see there are some very diffuse and aggregate consumer concerns. They are not site-specific. So it's not that consumers are not concerned. Indeed, they are very concerned. But when you start to look down at what's happening at the level of specific sites, there are some very interesting hypotheses that we have started to generate that are supported by some recent research suggesting that consumers are making decisions in real time about the privacy and security of a particular site.

What happens is consumers have these diffuse concerns, but when they hit a particular website they say, "Gee, is this particular site a safe one for me to be interacting with, or giving my information up, or shopping," or what have you.

And if consumers conclude, yes, this one looks good, then they proceed. If it doesn't look good -- and I will talk more about that in a minute -- then what happens is they will handle their concerns either by, for example, not giving information at some point to that site, making up the information that they actually give to that site, or just simply deciding, "I'm not going to interact here," and they leave the site, or they just do the minimum.

So, it's not really a paradox, then, this idea that these attitudes and behaviors are in conflict. But clearly, a lot more research is needed to probe these sorts of ideas.

And so what I want to do in just about the 10 minutes or so that I have left, is just briefly skim some of the recent research that is just starting to be done in the academic arena, which I think is fascinating, and hopefully can generate a lot more research coming down the pike.

First of all, I want to talk about some recent

studies on website credibility. The headline here is that if you ask consumers in a survey setting, they will tell you that objective factors are very important in determining the credibility of a website.

And just so we're clear on what credibility is -- because I think that gets confused a lot with the trust issue -- credibility is the belief that the website has the expertise to do its functions effectively. So, credibility means the website can do what it says it does.

If you ask consumers what makes for a credible website, they will tell you things that have a lot of facial validity and are very objective. So, for example, consumers will say that a website's credibility is one of the most important drivers of when they use a website. They will tell you that online shopping sites and online recommendation sites are the least credible, that the federal government and the new sites are the most credible.

Consumers will also say that they want websites to provide clear, specific, and accurate information so that will help them gauge the credibility of those sites, and that specifically means things like privacy policies, contact information, have a very clear statement distinguishing the ad from the editorial, and so on.

And then consumers will also say, for example, that search engines should indicate that there are paid listings, and they are using paid listing practices to decide the order or the ranking of the listings.

But if you look at that, what's really interesting there is most consumers have no idea these practices exist in the first place, and so you actually have to tell them that. And then you say, "So, now what do you think?" And they go, "Oh, okay. Well, I don't think I like that." So there are some problems regarding consumers' knowledge.

Then there is some other research done which actually tries to look at consumers' behavior with respect to credibility.

And remember, I have talked a little bit about this idea, that maybe there is this privacy paradox with respect to attitudes and behavior, and suggesting that it's probably not really a paradox, but we have to decide what level we're talking about.

And here again, we may see something that looks again like this paradox, because it turns out consumers don't really use any of those rigorous objective factors when they're actually trying to evaluate the credibility of websites. Instead, the things that appear to be the most important are the design of the site, usability

criteria, and the content scope. And that overwhelmingly dominates what consumers notice when you are asking them to judge the credibility of a website.

So, for example, the overall visual design of the site is the most important factor in determining whether a website appears to be credible. And that has to do with things like layout, the typography, the font size, the color schemes, how much white space, how many images, and so on. And sites for which this is the most important are financial sites, search engine sites, and travel sites.

The next most important criteria has to be the information structure. That has to do with the idea of how easy is it to navigate through the site, how is the information organized on the site, and so on.

And then finally, information focus, which has to do with this idea of breadth versus depth. One of the things the research suggests is that the depth of a site's content suggests a lot of authority in a website. Too much breadth, and the site is perceived to lack a very strong focus, and that seems to hurt its credibility.

Now, I think what's the most disconcerting about this stream of research is that very few consumers appear to notice the objective factors that are believed

to be important for improving online credibility.

And in fact, some researchers took the list of guidelines put forth by a number of different industry groups for improving credibility on the Web, but those are not the things consumers attend to.

For example, less than one percent of consumers in this study even think the privacy policy is relevant for evaluating credibility.

So, moving on, then, if credibility is a component of trust, and trust has to do with the consumer's willingness to rely on a website in which it already has confidence, then it makes sense to look at the bigger issue of trust.

And here, I am summarizing some research which shows, again, and supports some of the other work I have shown you and also a lot of work I'm not talking about today, in the interest of time, that web characteristics, other than privacy and security, are the primary drivers of trust on websites. And again, we see that how consumers navigate through the site, how easy the site is to use, is one of the most important characteristics of trust, as are the brand name and whether the site provides advice or recommendations, and so on.

There is some suggestion from this research that trust seems to depend on industry categories. So,

for example, financial services sites are seen as intrinsically more trustworthy than, for example, sports sites. But I think we need a lot more work there.

One of the things that's most surprising about this research, and is now beginning to come out in a lot of work in this area, is that consumer characteristics -- for example, how long you have been online, how much experience you have in the online space, whether you can assess a site's quality, how much education you have -- seem to play either no role or only a very small role in determining the trust factors. And so, I think that's a big difference from previous research in this area.

Now, finally, if we drill down and take a look at consumer behavior for a very specific task on a website -- in this case, the opt in versus the opt out task -- we can see here how this theme is repeated, this idea that relatively superficial factors appear to have much more influence on consumer behaviors than what consumers' attitudes are actually telling us.

And here, this stream of research is very interesting, because the idea here is the consumer's choice can be dramatically influenced by the default options.

So, for example, whichever option is pre-checked on the website, either it's "yes, I do want to be

notified," or "no, I don't," and how that's worded is the framing part of the question. Then what the default is -- whether an option is pre-checked and you have to remove it, or whether there is no check and you actually have to put one in -- that seems to have a dramatic influence on whether consumers will participate or agree to be notified for more information.

One of the interesting issues here is that consumers view the default -- in other words, whatever the pre-checked option is -- as the correct choice, or as the status quo, or the more popular one, and therefore, it must be right. And there is a lot of research from the cognitive literature and the decision sciences literature to support that idea. That's turning out to have a big impact on what's happening with the adoption of privacy policies. Framing the option is also well known to influence choice behavior. And so, there is an interaction here.

Now, let me show you, just briefly, some of these results. One of the things one study found was that a positive framing and a positive default yield much higher participation rates than negative framing and negative defaults.

And so, for example, with a negative frame, like, "Do not notify me," you get much lower

participation rates, than if you have a positive frame, which is worded as, "Yes, do notify me." And then the negative defaults have lower participation rates than the positives.

What's really interesting here -- and we need a lot more research on this -- is that the no default forces the consumer to make a choice and yields participation rates that are a little bit closer to the positive default than to the negative default.

The research also suggests that these effects are additive. And so, if you put the positive frame and the default together -- in other words, the yes box is already checked for "notify me," you get about twice as much participation as you do than if you have the negative frame in default.

And again, highly consistent with the trust research I told you about earlier, the online experience and education don't seem to have anything to do with the results. So this is not a situation where if you have a Ph.D. and you have a high income, you will be immune to these effects. This affects everybody, regardless of their consumer characteristics.

And again, this research is very consistent with research we are now able to bring in from other domains.

So, what does this all say? The bottom line here is that we already know that consumers are very concerned about online privacy. But recent research from the academic realm is beginning to suggest that people are more apt to use sites that are designed in a certain way.

In other words, if the overall look of the site makes it seem credible, then they think it must be credible. And it's not clear how these factors actually bear on a site's trustworthiness, or how they even demonstrate the protection of a consumer's privacy or security.

So, I think there are enormous implications of this kind of research, and a number of issues that are raised. There is a lot of complex cognitive effects at work that we just don't really understand yet, and we're going to need a lot more experimentation and research to understand them.

It's very clear that there are some lessons that technologists are going to need to take into account when they design systems to protect consumer privacy. But there is still a lot we need to know.

For example, we still don't know what factors are most important in encouraging consumer interaction at websites. We have some idea of the topline main factors,

but we don't understand how these factors interact.

We don't understand the distinction between opt in versus opt out privacy choices, and how they are most important in building credibility and trust, and how they interact with some of those other factors, like how the website looks, whether it has a brand name, and so on, and how these key factors might influence these privacy choices and interact.

And it's very clear from this privacy paradox idea that I shared with you a little bit earlier, that we need much more site and content-specific research, so that we can tease out the general concerns, and how they impact specific behaviors at particular sites. Thank you very much.

(Applause.)

MS. GARRISON: Thank you very much, Donna. Well, I hope everybody had their seat belts on for that one. That was terrific.

I would like to ask now that the rest of the panelists for panel three slide up here and take your seats.

Our three presenters now are joined by the following panelists to talk about the issues that were raised by these very provocative presentations. They are, from my left, Parry Aftab, a cyberspace lawyer

specializing in privacy and security, George Gaberlavage, who is the associate director of the AARP Public Policy Institute, Susan Grant, vice president for public policy from the National Consumers League, Jim Harper, editor of Privacilla.org, Tim Lordan, staff director for the Internet Education Foundation, and to my immediate right, Nat Wood, who is the deputy director for the FTC's Office of Consumer and Business Education.

I would like to open this afternoon's discussion with a question to all the panelists. We have heard today a lot of discussion about how people handle technology in many different ways. What are the lessons about how technology should be designed so that people can easily use it?

Parry, would you like to start the discussion?

MS. AFTAB: I would be happy to, thank you. I think that we start it from the wrong direction -- so far, the Internet has controlled how people interact with it, instead of people controlling the technology.

And I think what we need to do is -- it's wonderful to have the people who design the technology get it here, but I think it's now time for people to take over what it is we need.

And so, rather than have it be technology-driven, it has to be use-driven. Rather than asking

users, "Do you want this," just say, "These are various factors," making it easy for people. "Do you want people to have your personal information? If so, what kind of personal information are you willing to share?"

And instead of doing it in a checklist, just say, "There are sites that can give you special products that will deliver goods that we know you like. Do you want to make your information available to them to make that easier?" And I think it makes it so much simpler to make it practical, and have the needs control the technology.

Don't talk about how great the technology is, not a whole bunch of check boxes up front at the start, just easy choices that people can make, as to what they really need, and let the technology and the check boxes be done afterwards, underneath it, using wizards that get the users where they want to be. And I think that's part of the problem. We're making it way too hard for people, even smart people, and we're taking far way too much time out of their time online for them to make decisions about what they do next.

MS. GARRISON: George, do you have anything to add to that?

MR. GABERLAVAGE: Well, I think the Web design -- I just wanted to mention one study that was, in

particular, oriented to older Internet users. It was a Jacob Nielsen measurement survey, which basically compared the responses of two age groups, age 21 to 55 and age 65 and older, on a set of tasks: research, purchasing, and retrieval of information.

And they found, basically, that the older group had an average of 4.6 errors, compared to less than 1 for the younger group. And one of the findings of the study that I think is interesting is that the poor design really contributed to the poor performance, because the design did not really take into account the physiological effects of aging -- eyesight, precision of hand movement, memory issues -- and they made a number of recommendations on what could be done to improve this situation.

Also, we did a survey in 2000 on consumer preparedness for e-commerce. And one of the things that strikes me is that 4 in 10 of the respondents rated themselves novices, even though they may have had several years of experience working on the Internet.

Also, 46 percent of them said that they had fairly frequent difficulties with software applications. So, I think that those are issues that need to be addressed, because there is such a diversity of individuals on the Internet, and I think, from the

standpoint of older people, it's one of the fastest -- they have one of the fastest rates of use now. I think those issues have to be taken into consideration.

MS. GARRISON: George, you have that study available outside as a handout, is that right?

MR. GABERLAVAGE: Yes, it's one of the handouts.

MS. GARRISON: Okay. So for anyone who wants more information, you can pick it up at the table outside. Susan, you have something to add?

MS. GRANT: Well, first, I want to apologize for occasional coughing fits. I think I am allergic to spring, but it isn't SARS, I assure you. So it's okay.

MS. GARRISON: Well, that's a relief.

MS. GRANT: Yes. I want to pick up on what both Parry and George have said. I think that we have to remember that technology, in and of itself, is not the solution, that technology is merely a tool that can hopefully help people to achieve a certain aim, to help them do what they want to do.

And while the web credibility studies showing that people judge the credibility of websites more by things like design and ease of navigation than by who is behind them and what their qualifications are, while that's disturbing, that can be helpful to us in a way, in

thinking about how to present privacy tools as part of the design of a website, for example, privacy policies -- how to build in the information and the options that consumers may have as part of the attractive design of a website, and not as it so often is, just something that our lawyers made us put in, and there is a button to click on the bottom, and that will take you to it. That is not what is going to attract people to the information, or to use the information.

MS. GARRISON: That's a very interesting observation. I would like to pick up on the Web credibility, and the trust issue in general.

Mary, I wonder if you might want to comment a little bit about some of the trust issues that were raised by Donna's research. Does it, in fact, show that consumers really have a lack of understanding of the data that they're seeing, the information that they're finding on the sites?

MS. CULNAN: In terms of how to protect their privacy?

MS. GARRISON: Well, just in terms of their own interaction with the site, and the findings of trust and credibility, or lack of credibility.

MS. CULNAN: I thought that was actually very interesting, the fact that it's how a site looks. And I

have to say I was almost a victim of that myself, as I was buying office supplies online, and found a site, and it looked fine. I bought the stuff, they sent me the wrong stuff, and they don't have a phone number, it turned out. So I finally learned that's an important thing to look for.

(Laughter.)

MS. CULNAN: Anyway, so I will be disputing that charge when it comes in.

But seriously, I think that it's just really interesting. It shows, also, how little we know that things we think should be common sense and should drive behavior really don't. And I think, in a way, it's also sort of frightening that people depend on cues that can be so easily faked.

And we need a lot more research. And also we need to, again, educate people on what to look for.

MS. GARRISON: Parry, I wondered if you had anything to add, in terms of the people you work with who come to you with problems online. This whole issue about Web credibility, the fact that what is attractive to them, or what appears to make the site credible, and are therefore what consumers trust and use, are really factors such as the web layout and not more objective concrete factors.

MS. AFTAB: Yes, it actually has negative connotations. Although we can use it to try to deliver wonderful privacy messages, I will tell you that the people who are out there conning people on the Internet already read this study. They know that they need to come up with colorful sites that look professional and are well laid-out, and they do that because they know people are going to trust them because of it.

But what we're finding is that the people who want to break the law and con people and hurt people on the Internet know an awful lot more about this stuff than most of the legitimate businesses do.

So while we're hoping that legitimate businesses will learn that their sites need to look a certain way, and whether the default mark needs to be there or not, and you hope that their lawyers and risk managers and marketing people are going to be advising them, people need to recognize that there are a lot of con artists out there who practice looking legitimate. That's the only way they're going to get your money.

And so, people need not to judge based on that, they need to judge based upon the other things. And hopefully programs such as TRUSTe -- and I'm on their board -- and BBBonline, and I love them, even though I'm not on their board, and a lot of the other programs can

be helpful. We have to start educating people to look beyond the coloring of the site and how well laid out it is, and look to credibility that's been -- that the tires have been kicked on, to make sure that they really are credible.

MS. GARRISON: We have heard a lot about technology and what it can do. We have also heard a lot about the need for education. If technology can't address all the issues related to protecting consumer information online, what are the limits to what it can, in fact, do? Mary, I wondered if you could take that one.

MS. CULNAN: The one thing that technology can't do is -- from the consumer's point of view -- is it can't change any of the company's information practices.

It's basically a company can give you a notice, you can make choices based on that, but then it's really out of your hands. And so I think people need to understand that limitation.

We can't oversell the technology to consumers, and lead them to think it's going to do everything for them. They really do have to be active in understanding how it works, or they're going to get fooled.

MS. GARRISON: Tim?

MR. LORDAN: Jim actually had his flag up

before.

MS. GARRISON: A true gentleman. All right, Jim. Please, go ahead.

MR. HARPER: The limits of technology are substantial. In an e-mail to Privacilla list members yesterday, I said that the most important privacy protecting technology is the human brain.

And I actually got e-mails back from the Hill saying, "This is interesting, this brain. Tell me what you find out about it tomorrow."

(Laughter.)

MR. HARPER: But real briefly, I want to try to characterize what I heard this morning, and in the panelists just now. That actually goes back before I was really working on privacy, when I was working on regulatory matters. Risk assessment and cost benefit analysis -- several people have mentioned cost benefit -- but consumer risk assessment and consumer cost benefit analysis are a way that I characterize this process.

They are happening essentially in real time. I think that's important to note -- Donna mentioned that consumers are making these decisions moment to moment -- they are saying, okay, what's the risk from this behavior, and then they do a brief cost benefit analysis between some choice of different behaviors.

And that suggests, really, two inputs that will affect consumer behavior. One is more information about risk, and the other is easier, easier, and easier privacy and security tools. So I think it is the brain, we are trying to affect brains here, as much as using technology. And here are some of the risks that privacy and security are in competition with.

I mean, just look at the paper, SARS -- I have a new concern about SARS just now -- terrorism, heart disease and cancer. These are remote, but real threats to people's lives.

Privacy and security are also remote but real threats to people's lives. There are two instances I know of where information was an important part of a murder. So they are on the same scale, but in different places on that scale. Educating people more about the risks, and obviously, making the solutions easy are the two points where I see benefits, going forward.

MS. GARRISON: Thank you. Tim?

MR. LORDAN: I actually agree on that brain thing. I think that is an up-and-coming tool that we want to use a little more.

(Laughter.)

MR. LORDAN: I heard Parry say something very consistent to that in the past, when it comes to safety

and other issues.

I feel more comfortable talking on the security issues in a lot of ways, because there are bad people out there, and they want to do harm to certain people. There are some really simple, clear messages you can communicate, which the Federal Trade Commission does very well at ftc.gov/infosecurity, and articulates it best -- use anti-virus software, install firewalls, et cetera.

And it seems like the spectrum of calculus -- the comprehension, as Andrew referred to it, I believe, that calculates what am I concerned about -- what are the fears, what's the education that I have had, am I concerned about people hacking in, am I concerned about getting an e-mail virus -- it's a very limited calculus.

When you go into issues like privacy, the calculus and the education, and that initial comprehension metric that Andrew articulated, it is massive. But for either information security and privacy, technology can't do it all.

But I will take issue with something Andrew said, that P3P has something like 36,000 permutations, or something like that. I have actually heard people say it doesn't have enough. But from the consumer perspective on what you get, it's really up to the tool manufacturer.

Let me give you an example, Lorrie Cranor's

Privacy Bird. We have three types of birds, one is red, not very happy. One is green, he's happy. That's a translation of those 36,000 permutations that you're talking about. She also has in there, "Don't send me unwanted e-mail." That is what the consumer sees. The consumer doesn't see those 36,000 permutations. They don't have to.

If the tool manufacturer makes a really good product based on the information that websites are disclosing in a machine-readable format like P3P, it can be incredibly powerful, if done right.

Back in Netscape 4, or Internet Explorer 4, back in the old days, you had three options when it came to cookies. You could say no to them, you could accept all of them, or you could say, "Well, I will accept them, but notify me," which turned out to be like that game at the fair, whack a mole, and you would be browsing, and all these windows would pop up, "Do you want this cookie," and you say no, and literally, it was like a whack-a-mole situation.

Evolutionarily, we're in Internet Explorer 6, and Netscape 7, I believe, Opera 6, and actually Apple just came out with one, too. And the interface for cookies is far more advanced.

Actually, Microsoft and Netscape took P3P

specifications in a certain way, and made some of those choices easier. And for that matter, they even made some default decisions for people based on some of the fine work that Toby and the Federal Trade Commission did with the network advertising initiative on merger of your click stream data with personal information that they might have gotten offline.

So, I think tools can accomplish a lot if people all buy in, but they can't do everything. The brain is an important calculus there, too.

MS. GARRISON: Susan?

MS. GRANT: I want to express some concern over people being manipulated sometimes, however, and I will give you an example where in a privacy policy, the options that consumers may have -- "yes, I will allow my information to be shared," and so on, is pre-checked.

That may be more effective, in terms of a higher number of people ending up allowing their information to be shared than not, but it doesn't necessarily mean that that reflects what people truly want. It's a manipulation for marketing purposes.

So, while I said before that I think that design is really important in making this technology work for consumers, I also think that consumers have to be respected. Design shouldn't be used in a way that

manipulates them, where they may either not bother to read something, and just by default end up agreeing to something, or where they somehow think that because it's pre-checked, that is the right response.

In fact, I think that maybe with security, some things ought to be automatic or pre-checked, but with privacy, I really think that people should be obliged to just say yes or no without any pre-checking going on.

MS. HOFFMAN: Yes, I --

MS. GARRISON: Donna, do you want to respond?

MS. HOFFMAN: No, I think that's a great point. If you think about this from the consumer's hidden true preference, their hidden true preference was probably best reflected by an opt in. And so this research is beginning to show that the best strategy is one where you force the consumer to make a choice, and so that there aren't any defaults.

And the reason is because -- I don't really like the word "manipulation," but clearly, consumers' preferences can be swayed by factors that really don't have to do with what their underlying true preference is.

And given that we know that, that suggests that best business practices are those which ask the consumer, "What would you like to do," and force the consumer to say, "Gee, what would I like to do," and that raises some

of these issues. If we're going to use our brains, well, then we need a little bit more education and notification on, well, "Help me decide what I should do." That means we have to have full disclosure, we need informed consent, we need easier, more attractive privacy policies, and so on. But you know, I agree.

MS. GARRISON: Andrew, based on your research in this area, do you -- and especially in light of this afternoon's discovery of the brain as a brand new tool here -- do you have anything else that you might want to add as to what the limits of technology are?

MR. PATRICK: The brain is a wonderful thing, but I don't want to let the technologists off the hook. I think a lot of the solutions are in the technology. I think we haven't explored at all what technology can do in terms of supporting those human requirements.

Technology is a very powerful tool for supporting comprehension. Technology that explains things to people, that provides the kinds of details on demand that may be necessary for people to understand concepts, provides the kind of control that people can use. And technology can lead people to good behaviors by making software that's easy to use.

So, although technology can't do everything, it's not doing anywhere near what it could be doing. It

could have good user-centered design, and really understand what it is that we're asking the users to do, and support them in doing it.

MS. GARRISON: Thank you. Tim, you have one more closing comment?

MR. LORDAN: Yes, just one last thing. With regard to the technology, what can it do, when it comes to notice, the World Wide Web, and even software for that matter, technology can provide a lot of really innovative ways to provide a consumer with notice.

Obviously, it has to be well-written, and it has to be sincere, and not try to manipulate people, but certainly, I think Marty Abrams talked about the layered notice project earlier and that concept of layered notices, where you get a simple, straightforward statement, and then obviously, you can go for more detail, should you like.

But the medium lends itself and the technology lends itself to providing better notice than you maybe get in a restaurant, or at the department store. And I think that's really worth noting.

MS. GARRISON: Thank you. Nat, what are the steps that consumers can take to help themselves protect their information?

MR. WOOD: Through discussions like this, we

have put together what we consider a consensus list that we're planning to review over time. And so if we learn today that there are other things that we should be concentrating on, we will be interested to do that.

We are putting up on the screen some of the tips that we have come up with. The two most basic have to do with passwords. Use both letters and numbers, and make them at least eight characters long. Use up-to-date anti-virus software. This is also very universal. We want people to use the up-to-date anti-virus software, and update it regularly. These tips are useful for, really, everyone.

For people that use broadband access, which is not yet everyone, but it's growing, we think it's very important to use a firewall.

In sending or receiving e-mail attachments, there are steps people should take. One is don't open an attachment unless you expect it, or know what it contains. And the flip side of that is if you're sending an e-mail attachment, type a message explaining what it is.

And we also want people to know who to contact if they have problems, and that could be an ISP or a software vendor.

MS. GARRISON: Great, thanks. Does anyone have

something to add to that list? Tim? Go ahead.

MR. LORDAN: No, I don't have anything to add to the list, I have something to add to the comments.

MS. GARRISON: All right, go ahead.

MR. LORDAN: Well, I think that list is really tight about information security, trying to prevent the bad things from happening to you.

And I think there is a lot that everybody can do, and I don't want to steal Nat's thunder on this, but there are a lot of things that businesses can do, consumer groups can do, privacy advocates can do. There should be no shortage of places on the Internet where consumers can find this information beyond just Google searching.

MS. GARRISON: All right. Susan?

MS. GRANT: Well, I think those tips are great. We stole them, and we stole the tips from the Internet Security Alliance to come up with our own six steps to computer security, and I put out a sheet on the handout table of the privacy resources that are available from us.

But having said that, Mary makes a good point about the importance of social marketing here. It isn't enough just to tell people that they should do something because it's a good thing to do, or a wise thing to do.

They have to see the benefits of it to themselves in a way that relates to how they see themselves.

And to do social marketing, which I think, really, is important here, to get people to actually use this technology, is going to take a big effort, an effort that really needs to be supported by the private sector, as well as government, because it's going to take a lot of resources.

You need to have an understanding of your audiences, and they are different because not everybody is the same, so you have got different segments of the population that you need to target your messages to.

You need to figure out what resonates with those particular people, and I think this is a real challenge, especially with security, which, as somebody said before, is so much harder for people to really see unless they happen to get a virus on their own computer. You know, the ramifications are usually not something that's going to be really obvious to people, and so it's going to take a sustained, concerted campaign to do this, the same way that we did a campaign some years ago about seniors and telemarketing fraud.

We used studies, we had a retreat of experts, we used focus groups. And a lot of time and a tremendous amount of money went into fashioning new messages to use

with different segments of the senior population. And I think this is a similar challenge.

MS. GARRISON: George? Do you have something to add?

MR. GABERLAVAGE: Yes. I agree with Mary about the idea of social marketing. I couldn't disagree, since Bill Novelli, our CEO, is one of the foremost practitioners of social marketing, being the architect of the Tobacco-Free Kids Campaign.

But I had my own personal experience with this in working on electronic funds transfer, and trying to convince older people, particularly the unbanked, that this was a good idea for them, that it protected them, and many of the same issues of trust were involved in that.

You have to develop -- you have to look at the market segments and develop messages for those particular audiences. You have to find different venues. Some of the research on seniors, for example, shows that if you can link a new technology with a particular utility for them, and link it directly -- for example, EFT was linked because it was a safety issue -- they will adopt it, as opposed to, say, ATMs, which have not been well adopted because seniors don't see the utility in it.

Also, certain types of marketing tools like

print media are much better for the older population. We have a lot of materials, and I put some of them out on our website. We have a number of fact sheets that deal with security issues, safe cyber shopping. We have the safety net, how to safely use e-mail, learn the Internet.

And we have a tutorial on our website, which I think could be very useful. It's called "Ask Sandy," Sandy is a consultant who is a very nice lady, and it explains things like cookies, browsing, bulletin boards. It discusses those kinds of things.

I think those kinds of tools may be the kinds of tools that could be used to promote the kinds of safety procedures that we want to encourage. And I personally -- I am always amazed at how quickly people pick it up, particularly older people will pick these things up, with a little bit of coaching.

I'm not so cynical as to believe that they are going to be fooled all of the time. I think if you give them some information -- and our experience -- Susan knows that AARP has worked on telemarketing, for example -- and I think that has been a very successful effort, where you have a message and you promote it in various venues. People do pick that up, and I think that is one way of getting this job done.

MS. GARRISON: Thank you. Jim?

MR. HARPER: Parry, do you want to go? Did you have something before me?

MS. GARRISON: Oh, you are going to defer to Parry for the moment? Okay.

MS. AFTAB: Go ahead, and I will do it secondly. You might come up with another brain comment.

MR. HARPER: Along with social marketing, I think plain old commercial marketing is important to keep in mind. I noted Mark's comment this morning that it was because of an advertisement for a paper shredder that his household now has a slightly more identity-fraud preventative practice of shredding garbage before it goes out. That's another key element -- folks who are trying to make money.

ISPs are doing a better job of getting privacy tools and anti-spam tools out there, and they advertise about them, too, and compete against each other on those terms, and I think that's an important piece of the puzzle.

MS. GARRISON: Parry?

MS. AFTAB: Well, in my non-profit life, you know, I practice privacy and security law and do consulting, but then most of my time is spent protecting people on the Internet, and I have got 10,000 volunteers around the world, all unpaid, who help me. And what we

have learned is any time anything goes wrong, we're going to get lots of e-mails.

Either people know everything, or think they know everything, or they know nothing. And everything in between is up for grabs. So what we need to do is find out what the real questions are. We think we know them, sitting up here, and we may do studies. We just went out with video cameras, and we talked to anybody who would talk to us, and said, "What are you worried about on the Internet?"

Pop-ups, pop-unders, and spam were the three most important things, and they asked a question, "How do I stop it? Where do I go? How do I report it?" So, number one is addressing the questions that already exist.

I think the second most important thing we can do is teach them how to ask the questions. When you talk to people about what information has been collected and what the defaults are, and the kind of technology that's available to grab information, people are clueless about this.

MS. GARRISON: So, Parry, how do we create more awareness?

MS. AFTAB: What we need to do is we need to take it away from technology and back to normal terms.

We need to explain that anti-virus software is the door to your house, and the firewall is the lock. You need them both. Most people have no idea what the differences are.

We need to explain that there are risks, that there are people who are going to try to get into your computer. If you don't have a really nefarious adult, you're going to have your kid's friends who are going to try to get into your computer. Explain what the real risks are, and that there are certain things they should be worried about, and there are certain things that they really don't have to worry about.

Cookies have gotten so much attention because people don't really understand what a cookie is. So when you're talking about cookies, "Oh, I don't accept cookies." "Okay. But do you have a firewall, and do you use an anti-virus?" "No."

So, what we need to do is separate the truth from the chaff -- the wheat from the chaff -- we need to say, "These are important issues. These are your options. This is what's going on that you have no idea is going on. So now, you have some choices to make, and you can implement those."

And people themselves are going to start making demands. And part of this issue -- and it goes back to

all the fights Tim Lordan and I have had over the years together on Internet safety issues.

MR. LORDAN: Not against each other.

MS. AFTAB: No, no, not against each other, next to each other on this one.

(Laughter.)

MS. AFTAB: Because in the beginning, when we looked to the ISPs to help educate people on Internet safety for children, we got a big pushback. They wanted to talk about the value of the Internet for children, but they didn't want to scare anybody, because they were afraid it would affect the adoption of the Internet in households.

Well, we're beyond that now. There are still some hold-outs, but now everyone recognizes the values of the Internet. They recognize the importance of e-commerce, they know they can get this information 24/7. Now we can risk letting them know that there are some problems, there are ways of being abused, and these are the things you can do.

And I think the ISPs and the ASPs and all of the OSPs, and everybody else who are out there need to commit to educating people on these issues, and what the issues are and how they can deal with it. And if they need one-to-one help, they can come to us at

WiredSafety.org. There is my ad.

MS. GARRISON: So, today we have been hearing that there are some fairly simple steps that people can take, but they are not taking them, to protect their information.

There is clearly a need for educational initiatives. Does anybody want to speak more to those? Mary, are you working with the Massachusetts AG's office on a project here?

MS. CULNAN: I am working with them. We haven't started anything formal, but we did have a conference last December that was largely motivated by the FTC's 2002 workshop, to start thinking about what we could do in Massachusetts to work on this problem, since it's so big it can't be solved in one big, fell swoop. And Orson Swindle was our keynote speaker, and we were very happy to have him there.

I think -- using virus software as an example, most people understand you need to protect your computer against viruses, even people with low technical literacy. But I don't think most people realize there is a new virus created every 12 seconds. And so it's not just loading it on. And if they knew, I think they would update it, because it's really not that difficult to do.

So that's one thing -- there needs to be some

easy ways to get this message in front of people. And think back to some of the campaigns that have been run here in Washington.

Channel 9 has, you know, get-a-buddy, where every 9th of the month, you call your friend and make sure you don't have breast cancer, or these kinds of things. Or you could get something clever -- a sticker that came with your computer that you could paste on the screen to remind you to update your anti-virus software on the 1st and the 5th, whatever is an appropriate frequency to do that, might help, for example, a big red card or something that came in the box also, to get people's attention.

People typically don't read all of the stuff that comes with the software, but they might need something that would help them understand how they have to use the software.

I think -- let's skip ahead, because we're almost out of time, but I will make one more point about education. Teachers have a lot of inertia around teaching new issues, so I think one of the things to help move this forward would be if somebody would develop some model curricula, a module that somebody could just drop into an undergraduate course, for example, so everybody that's teaching this doesn't go out and have to figure

out what do I have to teach, what's the right stuff, how do I draw the slides, et cetera, et cetera, et cetera.

I think this kind of thing can be very helpful, and I think the software can help educate, also. I know one thing, until I got a firewall that started notifying me every time I was getting scanned, I didn't realize how frequently this happens, and it really can happen to you. And then it gets to be so annoying, it's like the cookie pop-up that you just turn it off.

MS. GARRISON: Okay, Nat?

MS. CULNAN: Turn off the prompt, not the firewall.

MR. WOOD: I think we want to use every avenue possible to make this about the consumers, and push these materials out. These groups have had a lot of excellent suggestions. There is a lot of great material out there.

I wanted to give a plug for some of our materials. And like many of the other groups here, they are free. We have publications, we have things like postcards and preformatted articles that people can use.

Dawn Holtz, who has been helping with some of the technical things here, is involved with her community newsletter. And her community is one of the most well-informed, I would guess, about information security and privacy issues, because she runs these articles over and

over again.

Putting information in product packaging and PSA campaigns, and things like that, are great goals. But really, there are things that just about everyone can do, no matter how small the group of people that you have access to.

MS. GARRISON: Thanks. Before we move to the questions, there is one last question that I would like to pose to the panel, and I would like Andrew, if you can, to open it.

The next two panels are going to examine the architecture of our technology systems, and designing in from the beginning into the architecture, managing digital identity and safer computing.

Andrew, based on the research that's been presented, the discussion that we have had here, what are the challenges that we, this panel, can give to the technologists and the companies that build these products to improve the state of information protection for consumers?

MR. PATRICK: I think the challenge is to remember that the technology is used by people, and that, therefore, using a user-centered design approach -- we heard about this -- or focusing on user's needs and addressing those needs is really important.

And there is a long history now of technology development that is focused on user-centered design and proper evaluation before it goes out the door. Many of the problems that we see in the usability and the security and privacy problems with much of the technology could be easily found with very simple user studies, or very simple market studies, where, before products go out the door, you actually sit people down and say, "Can you use it? Can you find the option? Do you understand this?"

It's not rocket science. There is a good 20-plus years of good user-centered design out there, but it seems that we have to relearn it all the time, especially in times where there are downturns, it seems to get ignored in favor of getting products out the door.

MS. GARRISON: So, good old fashioned consumer testing?

MR. PATRICK: Yes.

MS. GARRISON: All right, Mary?

MS. CULNAN: Changing the subject briefly, before we do the questions, I think we missed a real good opportunity this year. National Consumer Week, which I believe was in April, was supposed to be about consumer information security. Nothing happened.

And a lot of times this does get a lot of

attention. It's a great opportunity to go on TV, to put business people from the community out -- the National Consumers League had a nice piece in their newsletter, but I did a Nexus search and there was nothing. This is for the whole country. Nothing.

And the only thing I saw in the Boston Globe, which is where I live now, the FTC was shown talking about identity theft, and I thought, "Why aren't you talking about security, too?"

So I think for next year, if there is a shortage of themes, run that by one more time and really give it a blitz. Because it will get a lot of attention if it's done right.

MR. WOOD: I think that's one of the reasons why we want to push materials in every way that we can. We had a pretty good push this year, and we did see some results. Maybe it's not as much in Massachusetts as other places, but we want to continue to take every opportunity. And hopefully, there are some people here who will have a light bulb go off that maybe your organization can do a little bit more, and we would be happy to help.

MS. GARRISON: All right. I would like to thank the panel, and move now to questions from the floor. If you could state your name, please, before you

ask the question.

MR. LE MAITRE: My name is Mark Le Maitre. My question was about guarantees. Donna, you touched on this. I think you said most people want a guarantee that their data will not be misused.

My question is about what form of guarantee would satisfy, because I assume that that's what they're after. Just to drop three things in, are they looking for things like assurance that the entity that they're communicating with is who they say they are, which is Mary's problem of going to a website and not knowing quite who is behind it?

Is it that they want, from whatever transaction they're involved in, a record that accurately reflects what they had agreed with the other party?

Is it that there is somebody out there that is nominated as a dispute resolution mechanism, in case either party doesn't live up to their claims? Is it all of those?

MS. HOFFMAN: It's simpler than that, and probably much more difficult to achieve. The deal breaker for most consumers is they don't want the data shared or sold to third parties. That's what they are really talking about when they talk about guarantees.

Most consumers don't really have a problem

giving data on these websites, because they do want some sort of personalization or information back. It's easy if you remember my credit card, and you remember my shipping address and that sort of thing.

So, they are okay with that. But the problem is -- and I didn't talk about this -- but permission marketing has run amuck. And it's permission marketing, and then its close sibling, spam, that have created enormous problems, from the consumer perspective, and that's what has led to a lot of this wariness.

And so, this guarantee is more along the lines of, okay, I get that you need to know who I am, I need to give you my credit card data, you do know what I am purchasing, maybe I understand you're tracking my click stream, maybe not, but I am really not comfortable with this information leaving your vicinity. And that's more what the guarantee is about, because they know it's leaving, because it's coming back to them in the form of things they didn't ask for -- e-mails they don't know why they're getting them, offers they never asked for -- and so it's more about that.

MR. LE MAITRE: So, if I tie it back to a real world example, in the, say, the credit card industry, where I walk out with a receipt that actually states what both parties have agreed to do, I may not know the other

party, I just know they're part of a network. Do I have to walk out, as a consumer, to feel comfortable, with something tangible?

MS. HOFFMAN: The work we have done in our lab, and in the work that's been done by a lot of people in this area shows very clearly, consumers want a very clear, explicit, easy-to-read, seventh-grade level statement that says, "I am collecting your data. I will not use it for any other purpose than my internal specific marketing need that relates to the transaction I am engaged in with you now."

MR. LE MAITRE: So it ends up being no more sophisticated --

MS. GARRISON: Okay, Mark --

MR. LE MAITRE: -- or no less sophisticated than a credit card receipt.

MS. HOFFMAN: Something very straightforward and simple, not, you know, a lot of pages with legalese and written so you need a Ph.D.

MS. GARRISON: All right. Thank you, Mark. Stephanie?

MS. PERRIN: I think my question is targeted at our researchers, down at this end of the table. And it concerns superficiality.

I think from a social policy perspective, it's

not a good thing in a complex world that we are aiming towards more superficiality. My take on your research seems to indicate that the Internet is really facilitating a very superficial response. If the box is ticked, you go with the ticked box. The web design is focused on less and less information, faster click through, and it does seem to me it's more like advertising with instant fulfillment than it is a richer shopping experience for consumers.

And I invite the consumer advocates to comment on this, because it could facilitate better research when I'm buying a computer. It could lead me to check what kind of firewalls or bundling could do this. It tends not to.

Have you done any research on where we're heading with electronic commerce on this whole thing?

MS. HOFFMAN: Well, first, I think I should clarify in the trust research and in the credibility research that I summarized, actually, the information scope is the third most important factor.

So, there is a very important depth component, and consumers do say that if the depth isn't focused, then it doesn't look credible. So I think one of the things you said is not exactly correct. Consumers do, in fact, appreciate that depth of information and that very

specific content affect credibility.

It's when it doesn't look focused, or it's kind of all over the map that credibility is affected. But at the same time, they are saying, "Could you make it easy for me to get around and find this information so I don't feel like my head is going to explode when I go to your website?"

MS. GARRISON: May we have the next question, please?

MS. WOODARD: My name is Gwendolyn Woodard. I won't mention the name of the e-mail software. However, when you hover over an e-mail, a lower window pane opens to let you see what is in the e-mail. And are you vulnerable to viruses under those circumstances?

PARTICIPANT: One of our --

MS. WOODARD: You know which one I'm talking about?

MR. PATRICK: It depends on the settings of your e-mail software. If you have it set properly, it will protect you when you're doing the preview of the e-mail.

MS. WOODARD: Okay.

MR. PATRICK: If you don't have it set correctly, you are not protected.

MS. WOODARD: But I think the way it comes,

that's the default in most of the e-mail packages that you get. And then a lot of people, like you say, don't know that, and once you look at -- you hover over it, and you look at it in the lower window pane, are you vulnerable to viruses?

MS. AFTAB: If you are using a good anti-virus software and it's set up to protect you against viruses that come in, it's going to catch it before you preview it in a pane.

MS. GARRISON: Dean?

MR. SHAHINIAN: Dean Shahinian. Very stimulating and enjoyable panel, thank you very much. I just had a question for clarification for the Vanderbilt research. You had mentioned, I think, that consumers are concerned about sharing their information with third parties.

If you asked a corporate lawyer, he might say a third party is any of the 2,000 companies that are not under common control, even if those companies under common control have totally different names, and are engaged in different lines of business than the one which the customer is dealing with and the customer has no knowledge of these other companies.

If you ask a consumer, they might say, well, a third party, "That's a company different than the one I

dealt with, and for a different purpose than I gave them my information for." I was wondering which, when you speak of the concern of consumers for sharing their information with third parties, what do you mean by "third parties?"

MS. HOFFMAN: It's the latter. The work that I'm talking about here is from the consumer perspective. So that's what consumers think of. And you know, their minds go back to the DoubleClick flap, for example, or something along those lines.

And so, the third party means I have a relationship with Company X, but then Company X turns around and, through its own relationships with Companies Y and Z, gives them some of my information and then I get information back from Y and Z. That's the main concern.

MR. SHAHINIAN: Thank you.

MS. GRANT: Loretta?

MS. GARRISON: Great question.

MS. GRANT: Can I respond to that?

MS. GARRISON: Susan.

MS. GRANT: There has been a lot of survey work about consumers' privacy concerns, and I really think the concern is broader than third-party marketing.

I think the concern is what the consumer reasonably expects his or her information is going to be

used for when they provide it for a particular purpose, and then what else might happen with it, whether it's by that particular company or somebody else.

So I don't think it's correct to say that it's just a third-party that gives rise to consumer concerns.

MS. GARRISON: Commissioner Thompson.

COMMISSIONER THOMPSON: First of all, thank you very much for coming. I thought this was a wonderful group of people talking about very interesting things.

It raised a couple of questions, and I think Susan sort of hit on one of them. Do you predict that we're going to see more of a trend in research asking people those open-ended questions about what makes you feel comfortable, instead of having a precooked series of responses that may skew our understanding of what consumers really want? That's one.

And second is that in the research you have done, how do you control for the question of mistake? In other words, your statistics are very interesting, but how does human error actually translate into some of those statistics?

MS. HOFFMAN: You mean like they didn't mean to check it, or --

COMMISSIONER THOMPSON: Right.

MS. HOFFMAN: Well, first, I should say –

COMMISSIONER THOMPSON: It's like saying --

MS. HOFFMAN: Right.

COMMISSIONER THOMPSON: -- "I accept" when you really don't know what you're accepting.

MS. HOFFMAN: Well, it brings up a whole host of errors. First, I should say that we have a lab we call E-Lab. Some of the other work I cited is also experimental work done in some other labs -- one at Columbia, and there is some work from some folks at MIT -- so the work is experimental, it's not survey work.

So you set up different situations, and then you manipulate some conditions, and then you see what happens. There are errors, but those can be part of the experimental paradigm. For example, consumers might not read a statement at all, and just keep clicking through. And that can be part of the experiment, and we do a lot of process measure, take response times, we do protocols at the end to find out did they read it, why did they check, did they make a mistake.

So, I think that can all be part of the process. I think it's pretty clear where we're going to go with our research, and the work we're doing with our colleagues is all trying to look along these lines at the no default setting. Under what conditions can we just force consumers to make a choice, and then what choice do

they make, depending on the environment around them on the page, and how it's set up, and how credible, and this and that.

And that's where I think there is going to be a lot of interesting work coming out in the next year, and then it's an open question, whether that will have any impact on business practice.

COMMISSIONER THOMPSON: Thank you.

MS. GARRISON: Well, I would like to thank everyone on the panel for a most stimulating discussion.

(Applause.)

MS. GARRISON: We will now take a very short break. If you could all please be back here at 3:00, there are cookies outside.

(A brief recess was taken.)

PANEL 4: BUILDING PROTECTIONS INTO THE ARCHITECTURE OF IDENTITY MANAGEMENT SYSTEMS

MS. GARRISON: It's 5 after 3:00, if we could ask everyone to please take their seats. Those of you in the hallway, could you come in and join us?

MS. LEVIN: All right, if we have everyone back in the room, I want to, first of all, introduce myself again for those of you who weren't here this morning -- Toby Levin, in the Division of Financial Practices.

And I am very pleased to have, as my co-moderator, someone who is very familiar to FTC proceedings, and I think to all of you who have been in the privacy space for any length of time, Richard Purcell. And he is going to help make sure that we have as provocative and as informative a discussion as possible this afternoon.

I then want to move just quickly to introduce the other panelists. The bios, again, are in your folders.

To my left, Michael Willett, followed by Brett Michaels, Danny Weitzner, Ruchika Agrawal, Loretta Garrison, my colleague, Ed Felten, Ari Schwartz, and Lynette Millett.

Now that we have had this discussion about consumer behavior and trying to better understand why

consumers do what they do, and the need for more consumer education, it's becoming even more clear, I think, that there is a real driver coming down the pike to get consumers to think about why privacy and security are important to them.

And that driver has to do with the topic of this panel -- building protections into the architecture of identity management systems. I would like to first start with having Richard set the stage for today's panel.

MR. PURCELL: Well, the question comes up pretty continually, why the heck would you want to be identified in the first place, and the issue I think that we are dealing with fundamentally here becomes one where we have to ask that question, "Why am I being identified? Why would I want to be identified? In what way would I want to be identified? How thoroughly would I want to be identified?"

And as we move into this technological world where there is ubiquitous computing, where there are new ways of establishing and holding identities and sharing that information, we have to compare that to the world we have today. And the world we have today pretty well sucks, as far as identity goes, because it doesn't work very well. There are very strong identity systems, but

they are not applied very well. There are very weak identity systems that are applied pretty broadly. It's kind of a mush.

And we have a schizophrenia in our culture today because, on the one hand, we have identity systems that share a tremendous amount of commonality, in terms of the identifier, the social security number and the driver's license systems, which are very weak, in terms of being protected in any way.

A lot of people in this room are probably carrying their social security number with them right now, for a variety of reasons that they have no control over. They have to, for one reason or another. We certainly have our driver's licenses.

The question becomes if that information is leaked or spread across the landscape, do we suffer harm, and we know today that identity theft uses those two features and the date of birth and the mother's maiden name, and some very weak kind of attributes of those systems, in order to conduct fraud.

Now, we are not very tolerant of that fraud today. We are very upset about it. Fine, we should be. On the other hand, when we begin to discuss ID systems that are strong, that are robust, we get kind of weak in the knees at the same time, because we start worrying

about the power of government surveillance and commercial enterprises using strong identity systems in our disfavor.

And the question becomes as we move into the digital age, how do we then get over this schizophrenia that we have where we say, on the one hand, I hate the weakness of our systems and the resulting fraud that's occurring in it, but I can't stand the idea of a new system that will become even more predatory over civil liberties.

So, which side of that argument you will ultimately fall on is important, or whether or not we simply begin anew at the moment we have in today in technology development, with design considerations that really work to make identity systems applicable to the business that we're conducting, and to the control mechanisms that we have been discussing this morning so thoroughly.

So, what we want to do today is to begin to talk about what does it take to design an identity management system in the digital age that actually overcomes some of the security and privacy issues that we see in this rather cobbled together system we have today.

And if you don't think that our identity system is cobbled together today, just look at your birth

record, your birth certificate, and think about how is it that I can get a passport based on a record, in my case, that's over 50 years old and has my baby feet printed on it, or something like that. I mean, I can get a passport on that. Is that a good thing?

Is my birth record connected to my marriage records? No, it's not. Is it connected to my death records? Well, no, not really. Who is the best possible source for identity theft? Well, it's a dead person, because they don't read their monthly statements any more. So, for a while, I can really take advantage of that person's identity, at least for a while.

It's because the systems aren't hooked together. Hook them all together, and we start freaking out about national identity schemas. So which way are we going to have it, is what this panel is partly about.

We would like, first of all, to talk about a study that will lay, we think, an enormously effective and helpful baseline, a foundation, conducted by the National Academy, and Lynette Millett is our first presenter.

MS. LEVIN: Again, the slides for her presentation -- also for Ari's, in terms of the content, following Lynette -- are in your folders. So hopefully you can pull those out to help follow along.

MS. MILLETT: Thanks Rich for that introduction, and thanks to the FTC for having me.

I was the study director for a project at the National Academy of Sciences that looked at the issues of authentication technologies and their privacy implications. And I should point out that Danny Weitzner, who is on the panel, was on that study committee, and he can jump in if I miss anything important.

Toby, and others on the panel have seen the pre-publication version of the report we produced, which was about 200 pages. Then we did a public presentation last month. I had a 50-slide slide deck. But don't worry, I only have four slides today.

I should point out that we will have the book some time this summer if you're interested. It's up online right now, but we will have hard copies later this summer. The title of it is "Who Goes There?" We almost titled it, "Who Goes There: Who Wants to Know," to indicate the challenge response of authentication and privacy.

As you might expect, identity ended up being an implicit theme in this project, and ended up coming out explicitly in the end. One of the NAS committee's major contributions was to come up with some design principles

to help people think about how to develop privacy-sensitive authentication systems.

One of the questions I want to raise that I think might be interesting for the panel to consider is when does an authentication system become an identity management system? So I don't think we actually use the term "identity management system," but I think there might be some interesting overlaps. And I think the terminology ends up being a key issue.

We wrestled with it a lot over the course of our two-year study. If you're talking in this space, you have to make sure you're all talking about the same thing, is basically one of our results. What do you mean by "authentication," what do you mean by "identity?"

So, what we point out is that authentication, identification, and authorization are all distinct. And in fact, there are many different kinds of authentication. There is identity authentication, attribute authentication, and authenticating an individual. And we have this long taxonomy in a glossary of what we mean by all these things.

But, for example, if you want to authenticate an attribute, an example is a ride at an amusement park, which says you have to be this high to ride this ride. It has nothing to do with who you are, existentially,

it's authenticating that particular attribute.

So, we did have the existential discussion about what is identity. We brought in books by Aristotle and Descartes, and we considered them, and then we decided to take a bit more of a pragmatic approach. So, for our purposes, an identity is only with relation to a particular system.

So, an identify of X is a set of information about an individual in a particular identity system.

So what does this mean? This means that people can have multiple identities, and that's okay. It's not fraudulent, it's not deceitful. Privacy is implicated when you start linking these identities across different systems. Of course, it can also have broad security ramifications, as well. Those are our main themes on identity. I am compressing those a fair bit.

We also talked about some systems issues. And again, one of our main points is that it doesn't matter so much what underlying technology you use, although it does, to an extent. PKI, biometrics, passwords -- although we tend to think that passwords are a pretty bad idea -- so while it doesn't matter so much what technologies you use, what does matter is how the entire system is architected and put together.

So the policy choices you make, the design

choices you make, your data policies, those will all affect privacy and security as much, if not more, than whether you have chosen PKI or biometrics.

So, we also issued a short report called, "ID is Not that Easy." It's not that easy after 9-11 about national identity systems.

Basically, that's the theme of our whole report -- that issues are not that simple. And simply saying you've got biometrics now so your problems are solved is not going to work.

One of the things you have to do is understand your threat model. Why do we authenticate? Often, it's for security reasons. So we need to have some access control, or we need to provide for some kind of accountability. So, understanding what the threats against your system are will help you decide how you need to design your authentication system and your authentication protocols.

Why are you authenticating, and do you actually need to authenticate? And if you need to authenticate, do you need to authenticate individuals? Do you need to authenticate identities, or do you need to authenticate attributes?

Related to this is the notion of secondary use, which we also spent a fair bit of time discussing.

Basically, the committee says that secondary use can be very dangerous, both from a privacy perspective and from a security perspective. I think that privacy perspective is obvious. If your system is being used for all kinds of things, then there are many opportunities for compromising privacy.

But the example we give for the security issue is to think about our favorite system, the driver's license system. I'm sure this isn't news to any of you that it used to be a driver's license was just to certify that you could drive a car on a public roadway. The DMVs know that it's being used for a lot more things now. It's used to verify age, it's used to let you get on an airplane.

And we point out that these secondary uses actually become dangerous, because the system was designed with a particular threat model and a particular usage model in mind. And now it's being used for all kinds of other things.

So what happens is if you think about our normal approach to security, which is we want to prevent attacks, we want to detect attacks if they happen, and we want to respond appropriately, well, what if there is an attack against a driver's license system, or something of that scale?

If it's used for so many things, we don't know whether it was a bunch of fraternity guys wanting fake IDs, in which case our response should be at one level, or whether it was state-sponsored terrorism. So, that's the extreme of why secondary use can be problematic, from a security perspective.

The last panel talked about usability. We also spent some time on that. User-centered design is very important, both from the prospective of the people who are being authenticated, and the people who are trying to manage and administer the system.

We have a very long chapter on government's unique and often constrained roles, when it comes to authentication. Government is a regulator, it's a user, and it produces our foundational identity documents, like birth certificates.

And I should point out if -- Richard, you mentioned the birth certificate and death certificate connection. There is one state, Iowa, that is trying to do this, to connect birth certificates with marriage certificates with driver's licenses with death certificates. It's an interesting approach. It only works if you stay in Iowa.

(Laughter.)

MS. MILLETT: But they are actually thinking

very hard, and I have been hearing some interesting things about that.

One of the things we get a lot of pushback on with this project is we make the very strong statement that driver's licenses are a nationwide identity system. I think I understand why there is such pushback on this. I won't try to explain the reasons, though, in case I'm wrong.

But this pushback actually reinforces our point. People will say, "We don't want to call it that, because it means bad things." But in fact, they are a large scale identity system. And as such, we think they should be subject to some of the questions we have put forward in both of our reports about how to think through, basically, privacy protections in these systems.

So, with all of that, I should also point out that when we discussed usability as the last panel recommended, we agree with them that education is also critically important for users to understand what's happening when they use authentication systems of various kinds.

So, one of our big recommendations -- there were many in this report -- but one of them was to say if you're thinking about designing an authentication system, here are some of the things you should think about in a

privacy-sensitive authentication system.

Essentially, this is a distillation of fair information practices, as applied to authentication systems. I am not going to go through each bullet here. Basically, we ask what are you doing with the data, who has access to the data, who is using it, who can correct it if there are mistakes?

As it turns out, what CDT has done with their authentication and privacy principles is perhaps a more concise and even better distillation of this -- I know that Ari is going to talk about that a little bit -- I think that our work is very complementary to theirs, and so I look forward to hearing more.

MS. LEVIN: I just realized that due to a high-tech stapling error, we managed to merge the NAS presentation with part of Lorrie Cranor's presentation. So in your packets, I believe, the additional page is part of Lorrie's earlier presentation. I apologize for the lack of brain power on that one.

MR. PURCELL: We highly encourage everybody to take time to go to the NAS site, look through this report, particularly the recommendations and findings, and read the report as soon as it is available in a printed form.

It is a very, very thorough work. It provokes

much thought about exactly how hard it is to do authentication, and why it's necessary to start over again, essentially, and not try to fix what is in our current system, but rather, using design criteria that's now newly established, to get going again on management systems, ID systems that work within this context that we have been talking about all day.

Now, one of the first points, as Lynette has pointed out, is that CDT has headed up an authentication principles effort to get a broadly subscribed platform for authentication put forward. Ari, can you help with this?

MR. SCHWARTZ: So, in your packet, the principles are this document here, that says, "Authentication Privacy Principles Working Group," and the principles themselves start on the second page. The first page is a little bit of a discussion about the process.

Before I go into the process, I wanted to thank the FTC as well, and the staff, and particularly Commissioners Swindle and Thompson for their commitment to the issue of privacy-enhancing technologies. It remains an important issue, despite the fact that the dot-com boom is behind us.

In fact, it's probably more important now, and

it's more difficult now than it has been. And I think this session, in particular, gets at some of the real complexities of the issue.

About a year-and-a-half or two years ago at CDT, we started having some discussions with many of the companies starting to build identity management systems. And we were starting to see that these identity management systems were being discussed in a wide variety of instances.

There was the kind of online uses of personal information, trying to make the consumer's experience on the Internet more convenient. The idea of using identity better in the physical space, questions of identity theft and fraud came up. Questions of national security issues came up. Really, just a whole gamut of issues started to arise in this national identity space.

And it turns out that identity is extremely difficult, and it is somewhat existential and difficult to grasp -- and I think Lynette did quite a good job of explaining some of the work and some of the difficulty that they had, in terms of coming up with terminology. We saw that very early on, that people were talking about the same thing, using similar words to mean very different things.

So, we wanted to try to get everyone around the

table. It took until about six or seven months ago, when we felt that we really could get people to sit down together, and that we were really at the crossroads at the time when we said, "Can we really build privacy into these authentication systems?"

We were at the point people were starting to develop standards, and we felt that that was really the time to start talking about some of these more difficult issues. And so we did what CDT does best, and tried to get everyone in the room together to vet these issues.

We had a good mix of certainly the vendors of identity management systems. Also some consumer-facing companies, some privacy groups, and some consumer groups, as well. And what we're presenting today is the interim report from this group. This is not meant to be the final product.

And in fact, I would like to get input from those of you who have not had a chance to look at this yet, and want to give feedback to it. I will go into some of the details of what we plan for the future afterwards.

As I said, we felt that people were at, generally, a similar point. I will just kind of paraphrase where we felt people were in one sentence, and then I will enumerate that with the bullet points in how

this worked.

People felt generally that authentication systems should be appropriate for each use, and the individual user should be given appropriate control and knowledge of the use of their personal information within these systems. These are my words, not the working group's words.

Now, that's a complex way of putting this issue, but I think that helps us. The basic idea is this is where we wanted to go with these principles, and try and break it out in a way that -- I think the NAS report did it in a much more concrete, "If you're doing this, here is what we recommend" kind of way.

We wanted to do more general principles that worked online, offline, and could work with the technology as things progressed in that way.

We first came up with our own vocabulary and ended up using the NAS vocabulary. After all, they were looking at Descartes, we were just looking at current uses of these terms. And we hope that the NAS terminology really does become the standard for talking about these issues.

One first point that I really want to mention about these principles is that we aim them specifically at consumer-initiated transactions and government

services. And by that, we mean interactions between a business or a government entity, and an individual consumer, or citizen.

And the reason we limit it to that area, is because there is a much different set of issues that happens in the workplace -- I'm sure we will discuss those in the June 4th meeting on business issues -- and also in terms of data mining and pattern analysis, things that are not consumer-initiated uses of that information. Another whole set of issues go on there.

And in fact, we have a separate working group that is dealing with the data mining and pattern analysis issues in a variety of contexts, and that's really just getting started. If you would like more information on that, I can send you to the right place.

But in these consumer-initiated transactions, and government services area, we put together these basic principles. We have limited it to two pages, which, I think, is about as small an amount as you can do with this particular topic, from what we found.

The first of the principles was provide user control. We started there because we felt as though it was important to say when you're dealing directly with the consumer, you should make sure that you get their informed consent. Lynn talked about secondary uses. In

that instance, in particular, the user control is extremely important. And I think Donna Hoffman's discussion of this issue highlights that as well.

Number two is support a diversity of services. This is more the marketplace discussion, in terms of supporting a diversity of services. Some people call this a federated model. I think it depends on the context of how this works.

Really, the idea here is that the consumer has the ability and has a range of choices that are appropriate for the particular use of the technology, and that they have choices within the technology, and there are choices of technologies.

We are trying to stay away from the idea that we should all have one number that we are going to use for many multiple purposes. Now, of course, if a user wants to take control and merge things back and make their lives simpler, easier, that's under their control. But they have the choice, that there is a marketplace is what's important here.

The third point -- and this is, again, something that Lynn pointed to earlier -- tries to make the point about this spectrum from anonymity to individual identity -- that there really are different uses of information that are appropriate for different

kinds of transactions.

Anonymity, pseudonymity, and individual identity, each have their place. If you are going to use individual identity, then you are taking on privacy concerns. And it should be only used where appropriate.

The fourth point is provide notice -- and all of these are tied together -- but providing notice is, of course, essential to helping to provide user control. But it's also key to make sure that it is a notice that the individual actually understands, that it's not seven links away especially in this type of a system, that it's actually at the time that the consumer is at the "teachable moment," as Marty Abrams was saying earlier today.

Fifth, minimizing the collection and storage. This is focused on the idea that when you take on personal information, again, it should be used appropriately, with the kind of transaction in mind, and that you're taking on extra privacy risks by pulling in more information and storing it for unnecessary or inappropriate periods of time.

And lastly, sixth, and the broadest bullet, is pointing out that companies should be following general privacy principles anyway, and should be accountable within those privacy principles. And that includes the

ability of an individual to access information held about them.

Now, in preparing for this workshop -- and really another reason I like the FTC is it was able to focus the working group and give us a goal of getting out an interim report -- we also tried to get a group of companies and groups to encourage consideration of these principles.

I do think that it's a diverse group. It's mostly the vendors of authentication technologies, but it gives you a sense of some of the types of companies that were involved in the working group, and we also had individuals involved. In fact, there are probably about 12 or 13 people who were involved who were sitting at the table. Some of them are mentioned here and some of them are not.

But if you would like to join, or you would like to work on the future of this report -- and let me first say where we're going with the future. The plan is to separate into two subgroups, one that focuses on the consumer-initiated transactions. How does this work for a consumer in the real world? How do these bullets play out? What are the scenarios, et cetera?

And then one for government services, which is a tricky issue, in terms of how information is shared

between government agencies, and how does it play out in that space, as well. And then we're going to combine it into a detailed report, and that will be the final report that will come from this group.

If you're interested on working on that in that working group, please contact me and we can discuss how you can get more involved. I am looking forward to getting some feedback on this, as well.

MR. PURCELL: Cool, thanks.

(Applause.)

MR. PURCELL: Thanks, Ari. We've got a 200-page report that gets very, very deep. Chapter seven is great, because it's the tool kit. Everything leads up to the fact that deployment is everything, and the tool kit in the report from NAS lays out a very good process by which -- or the considerations for a process upon which authentication is built would be conducted.

Ari has got two pages of the principles that would underlie that process as a set of principles, design considerations that are fairly tightly scripted, and work, we think, across the conditions that we have been describing today.

But part of this is data minimization, part of this is, "Geez, why do we do this?" Why isn't the problem here that we just do this too much, anyway? That

maybe just not authenticating, maybe just not collecting information is the best way to proceed in terms of protecting privacy. And there are certainly arguments on both sides of that.

Ruchika, I wanted to ask you the question, is it not true that data minimization is just simply overlooked as one of these principles? I know it's in the principles that Ari is promoting, but it's not generally in the authentication protocols that we see today.

MS. AGRAWAL: I think that's right, because even the NAS report discusses authentication in terms of access control and accountability. So I would agree that minimization of the collection of personally identifiable information tends to be overlooked.

MR. PURCELL: So, where do we go? I mean, how do we take these principles? Do we have a reasonable expectation that these principles are going to be used as baselines and foundations for the development of new authentication technologies and identity systems, as we go forward?

MS. AGRAWAL: The NAS principles?

MR. PURCELL: Yes.

MS. AGRAWAL: Okay. I actually want to take a step back, and I'm not really going to answer your

question directly. But from this morning's panel and this afternoon's panel, I want to take a step back and just talk about rethinking through some of the things that we're discussing.

Just start from scratch, forget that we have spent all this time, energy and money behind some of these issues, and just start thinking about things from scratch and ask ourselves what problem are we trying to solve?

Are we trying to solve the protection of personal identity? And if so, what does that mean? How do you design an architecture that respects that, that supports that? I will briefly comment on P3P.

P3P translates a privacy policy into ones and zeros, it doesn't improve a privacy policy. I think there is a role for law and there is a role for technology. And I think that their roles are complementary. One really can't substitute for the other. So that's my comment on that.

And as far as the authentication report, there are lots of issues, and I want to fulfill my role at a public education forum and talk about some of the aspects that weren't discussed in this report. And it's a big body of expertise by Dr. David Chaum, Dr. Bronze. There is an underlying conception of PKI, and that's another

level that needs to be reworked and rethought out.

And the privacy problem that we're confronted with is that with our current PKI infrastructure, you have unique digital certificates. And whether you're talking about attribute authentication, or generally digital certification authentication, they are unique.

So, the main point that I took out of the report was the recommendation that you need to change how the PKI infrastructure is used. I think you actually did step back and rethink through the whole PKI infrastructure, and that's going to be my indirect response to your question, Richard.

MS. LEVIN: And why do you mean re-think PKI?

MS. AGRAWAL: Because the underlying fundamental problem, with PKI infrastructure right now, is you still have a unique identity.

MS. LEVIN: So you're suggesting the first question should be do you need a unique identity in any of the architectures?

MS. AGRAWAL: Well, I guess this would be a research agenda question. Can you architect PKI so, for example, for attribute authentication, you can have duplicates that if you're over the age of 21 -- I am over the age of 21 -- we can have the same certificate.

MR. PURCELL: That isn't trackable back to an

identity.

MS. AGRAWAL: Well --

MR. PURCELL: So what you're saying is that it's not connected, necessarily, to the identity, right.

So, an attribute, of course, isn't unique. Most people in the world -- you know, there are probably a few million people at a certain height, they're a certain age, or whatever.

The question is if I carry an attribute identifier that may be quite encrypted and secured, the problem is it still tells something about me as an individual, rather than just being an attribute that I share with any million of individuals.

MS. AGRAWAL: Within the PKI infrastructure, yes.

MR. PURCELL: Right, right. Interesting. Good. I think we may be able to get to that. Michael?

MR. WILLETT: Well, I had a comment.

MR. PURCELL: Yes?

MR. WILLETT: And let's not really fault PKI for this shortcoming. It's probably the way it's implemented now. But the basic role of a certificate in PKI is to bind an entity identity to a public key.

In other words, there are extendable certificates for other parameters, and so on, but I am

binding an entity to a public key. And that entity does not have to be an individual.

MR. PURCELL: Right.

MR. WILLETT: So it's not a public key technology problem, it's perhaps the way it's implemented in some context, where you are binding an individual, of necessity --

MR. PURCELL: The way it's actually implemented, then.

MR. WILLETT: Right.

MS. AGRAWAL: The fundamental problem is that the public key is unique, and that's all I'm trying to say.

MR. WILLETT: That's just the nature of the mathematics, though.

MS. AGRAWAL: Okay.

MR. PURCELL: So, let me make sure --

MR. WILLETT: Public keys and private keys are keys, and --

MR. PURCELL: Just for myself, as much as anybody else -- the scenario is I go to the post office, and I say, "Hey, look. I am 21, I can prove to you I'm 21. I am over 21." I mean, that's easy. I haven't been carded in a while, it's a bummer.

(Laughter.)

MR. PURCELL: So, I can prove that to the post office. And they can give me a key credential, a credential that says I'm over 21. The question is -- PKI allows them to do that without creating an identity for me, and tying that to my identity, necessarily.

MR. WILLETT: That's right.

MR. PURCELL: But some implementations that we see today overlook the fact that it can be unbound from the identity, and they bind it to the identity, which is objectionable.

MR. WILLETT: Well, it's the nature of the application. As a client to a Lotus Notes server, you're an individual.

MR. PURCELL: Right.

MR. WILLETT: So it's just the nature of the applications that have evolved.

MR. PURCELL: Okay.

MR. WILLETT: It's individuals involved in an environment where they need to be certified and authenticated. When we want to certify pseudo-anonymous identities, the same technology would apply.

MR. PURCELL: So we want to get back to this in just a minute. But what I want to do first, before we do, is ask Danny a couple of questions, or just kind of turn him loose -- and those who know Danny, know that's

very scary.

(Laughter.)

MR. PURCELL: What we want to really think about here is who are you on the Internet. In the digital age, how do we treat people today, in terms of recognizing who they are.

Then we want to talk about how we combine "who you are" with "what you know," the password issues and others. We also want to flavor that in with the "what you have" as authentication mechanisms, and then figure out how that data is processed? Who is handling it, and where is it going, and how is it being used?

So, I wanted to start with Danny with the way the Internet today essentially recognizes who you are, and whether or not the old New Yorker cartoon about on the Internet no one knows you're a dog has ever had any veracity, whatsoever. Danny?

MR. WEITZNER: Well, those are hard questions. I have to say the process of working on the NAS report was a hard process. And actually sitting here, hearing it described and thinking actually about your initial questions, Richard, is it possible, even, to take enough steps back to start again with these principles between the CDT principles and the terms that we pulled out of Descartes and Wichtenstein. How do you even think about

this problem?

And I have to say, I am personally increasingly troubled about this. This is like trying to debug a payroll system that's already spitting out 10,000 paychecks a week, and saying, "Oh, well, the way they're coming out is not quite right, so we had better somehow stop this and go back and rethink whether we should even be paying our employees," and ask all these very fundamental questions.

We simply don't have this luxury. And it's very troubling, because I have to say, with all due respect to my colleagues on the NAS study committee, I think we only barely scratched the surface of questions, and frankly, had a very hard time even getting our hands around how to make practical actionable design suggestions. It was very hard, and --

MS. LEVIN: So, does that mean the technology is going to control, and the policy makers --

MR. WEITZNER: Well, no, no. I guess what I really want to say in answer to Richard is that there is just a huge amount of social and institutional inertia that is moving things along. So, the point that Lynn stressed, that we already have a national ID system. Debating about whether we should have it or whether it all could be anonymized, I think, is -- it's several

decades, if not several centuries late.

And I think we have to come very squarely to terms with that problem. We did get some comments during the process of the report that we didn't pay enough attention, for example, to the sorts of anonymizing technologies that Ruchika referred to.

I have to say the committee was actually probably stacked with people, including myself, who were very sympathetic to that set of anonymizing technologies, and we, frankly, had a very hard time doing anything except to say what Stephanie Perrin said this morning, which was, "Well, that was a nice try. It's too bad it didn't work."

I know David Chaum will be here later, and I am sure he will have an intelligent answer about why it didn't work, but the reality is we have this world full of systems that are increasingly linked together, which really have been designed in complete denial of most of the principles that we're all going to probably sit around here and agree on.

So, I don't mean to be gloom and doom, but I guess --

(Laughter.)

MR. WEITZNER: I guess the point to take out of this is really that what we have in the physical world,

as you stated, is clearly a very intensive, pervasive structure of identification systems. Some of them already bleed online, some of them sit in records offices in your home town, wherever you were born.

And I think that, at minimum, what we ought to be enormously careful about is how we manage the transition from these existing systems to new applications online. That's where I think some of these principles can actually help. Rather than trying to say we can ignore the existence of identification systems that violate a whole series of principles, what we should do is be very careful about new applications of these systems, and be especially careful when we concentrate these identification systems together in places such as under the rubric of the U.S. government.

And I think the main reason to be very careful is because the identity systems that we have today, for whatever privacy problems they cause offline, they have a certain amount of flexibility to them. We all walk through this security system.

And by the way, Toby promised us that we wouldn't have to show our IDs; we did have to show our IDs -- but the reality is, I don't really care that much, and probably none of us cared that much, other than on principle, because we didn't, luckily, have to scan any

IDs. The guard looked at the picture and said, "Yes." There is no record of that kept. And these --

MR. PURCELL: We're coming in here to be taped.

MR. WEITZNER: Well, okay. That's right, that's right. But the identity systems that we have today that are, indeed, pervasive, at least have a certain amount of flexibility in their application.

As we move those identification systems to a more system-level Internet infrastructure, they will not be so flexible, they will be much more rigid.

MR. PURCELL: Right.

MR. WEITZNER: They will have to make on or off choices about questions such as, "Well, do you keep track of who came into this meeting or not," and the fact that someone left three times, or whatever else it was.

So, I think we have to accept the fact that we're in a -- what did they call the beginning of the Iraq War, a running start -- we are already very much in motion here, a rolling start. And I think that makes things very hard.

MR. PURCELL: That does make things hard. And I think one of the things that sticks with me as I worked for years and years at Microsoft, thinking that, well, technology will save us all, is the fact that technological developments don't tend to be very fluid,

in terms of pendulum swings.

Once they are in place, they stay in place, and they begin to be used for a variety of additional purposes outside of the purposes that they were put in place for. So that's where we get into some trouble.

I wanted to turn to Ed, and just say what's next, Ed? Lynette said earlier, and the report makes very clear that passwords suck. They're just -- it's a bad thing, right? I have challenged people in these kinds of meetings -- anybody here use encrypted e-mail with digital signatures?

Of course, I didn't at the time, so I dutifully went home and created my own account, and did all that, and sent out a series of encrypted e-mails, signed, just to prove to people that I could do this. And then about three months later, I tried it again and, of course, I forgot my password, because the two elements of good passwords, as the report says, are make it really, really hard, impossible to remember, and don't write it down.

(Laughter.)

MR. PURCELL: Great. So how do we get out of that mess?

MR. FELTEN: Well, passwords are an interesting situation. It's actually a common situation in security technology, where we have, on the one hand, a

sophisticated, exciting technology that's reasonably secure, and on the other hand, we have the lousy technology that we actually use. And passwords are that lousy technology.

The reason we actually use passwords, I think, is actually pretty simple. First, it's the simplest of all the authentication technologies. It's the cheapest and the easiest to deploy, the cheapest and the easiest to use, and you can use it anywhere without any special equipment or training.

Those things are not true of any of the other technologies. And so, there are, if not good, at least understandable reasons why passwords are used almost all the time. And passwords illustrate some of the difficult issues in authentication systems.

First, one of the problems with the password is that, like all of these systems, it doesn't really authenticate identity, it authenticates something else and uses that something as a proxy for identity.

In the case of passwords, it authenticates whether you know a particular thing, and as Richard learned -- as we have all learned -- the fact that you don't know that thing any more doesn't mean that you're not the same person.

And on the other hand, the fact that someone

knows my password doesn't mean, necessarily, that they are me. There are lots of ways that a password could be captured, passed along. I could divulge it through trickery or some other way.

And so, knowledge is not like identity, and using knowledge as a proxy for identity is dangerous, in the same way that using possession of an object as a proxy for identity has its own risks.

The other issue that I think passwords illustrate well is the proliferation of different identities that people have, or at least have the opportunity to have. Many different websites, many different institutions give you the opportunity to have different passwords. And if you stop and actually count how many passwords you have, the number is astounding.

I talked my wife into doing this. We went through this exercise where we counted how many different passwords she had -- different websites, ATM PIN cards, alarm decode codes, combinations of locks, and so on. The answer, in her case, was 144. You could count yourself, and if you actually count the websites you have been to, all the different secret numbers and names you have to remember, you will probably get into the same ballpark.

Now, the education programs say that you are

supposed to use 144 different passwords, they are all supposed to be hard to guess, and you're supposed to change them often. They also tell you that it might not be a good idea to use the same user name on those 144 sites. And so, those should also be different.

Now, in practice, nobody is going to do that. Nobody can. And education is not going to solve that problem, there just aren't enough brain cells in the world to deal with that. And even if there were, we would have better uses for them.

And so, the sheer proliferation of different uses of identity and different identity systems, which often are not federated, leads to a big management problem which we need some kind of technology to deal with.

I think, in some ways, the problems with passwords really reflect something Danny said, that not only is this not such a great technology, but to a large extent we're stuck with it because there are many sites out there that want to authenticate us by our passwords, and only know us by our user name and password. How we get from here to something better is an interesting question.

MR. PURCELL: But the fact that it's cheap means it has persistence in the marketplace.

MR. FELTEN: That's right. And not only cheap, but also very easy to deploy and use.

MR. PURCELL: Right.

MR. FELTEN: So it's hard to get rid of.

MR. PURCELL: So it's resistant to change.

MR. FELTEN: Absolutely.

MR. PURCELL: So, the problem is that for 144 different instances where a password is needed, a lot of people use the same password over and over, 144 times.

MR. FELTEN: Or write them down.

MR. PURCELL: Or write them down.

MR. WEITZNER: One illustration on passwords, and how bad the security is and how easy it would be to fix it and how unlikely that is to happen.

The HTTP protocols over which most people transport their passwords originally did not provide for any encryption mechanism for transporting passwords. So if you used SSL, you could have at least a safe transport of passports over the wire -- forget about all the other attacks that are possible. But the original HTTP protocols didn't provide that.

They now do, and there is a grand total, as far as I know, of one browser in the world -- which is actually produced as sort of an experimental project at W3C -- that actually implements this protocol. And it

would not be hard to implement. There are not that many different browser products out there. There aren't that many different web servers out there. This could be fixed really easily, but there is this extraordinary inertia, and kind of lack of incentive to even do something that would be so simple.

I think most people don't understand that when they do the normal user name/password combination on their web browser, that it's just going out over the Internet for lots of people to grab.

MR. PURCELL: Right. It's not HTTPS.

MR. WEITZNER: It is not HTTPS.

MR. PURCELL: Right, right.

MR. WEITZNER: So, anybody who wants to shoulder surf can pick up whatever they want at that point.

MR. PURCELL: That's right.

MR. WEITZNER: Keep in mind, SSL is great for preventing shoulder surfing at the ATM. Essentially, you can't look over somebody's shoulder and see what they're keying in.

The earlier comment was once it's in, God knows how it's stored. And so, it's the difference between pick-pocketing and bank robbing, robbing a vault. So it's easier and more productive to go in the vault. But

at least at this point, HTTPS is not deployed.

MS. LEVIN: And I'm just wondering, is this an example where we're always saying technology is moving too quickly, but why is technology not moving quickly in this area?

MR. MICHAELS: In the area of passwords? I mean, it's an interesting question. There is a lot of technology of many different form factors that are available today to provide a better authentication mechanism than passwords.

And it would appear that the actual business drivers are not there, or that the other business drivers are taking away from the issues of privacy concerns or security concerns. People are more than happy to focus on getting connected and getting into systems than spending money on the security or the privacy issues.

And you know, the technology is incredibly simple, in terms of its actual function. Perhaps the cost of deployment of it versus the business driver is the real issue.

MR. PURCELL: Right, right. Well, Ed, you talked about passwords, and how knowledge is a poor substitute for identity. You also mentioned that an artifact is a poor substitute for identity, as well. But I am going to ask Michael to give us a little bit of

feedback on that.

Now, Michael took the Donna Hoffman speed deck presentation course, apparently, because he gave earlier today a very, very quick overview of PKI, which is confusing enough slow. So you might not have gotten the whole thing. But the question here, really, is not the technology so much, but what's the application of artifacts, in terms of what you have that can help to establish -- or at least to authenticate, if not to identify you.

MR. WILLETT: Okay. And the article I'm focused on, in particular, is the smart card. But what I want to do is point out that I included in the packet you have a one-sheet background piece for this panel.

For your interest, by the way, you might look at the last chart on that, which is the Oasis committee, one of the standards committees in XML has standardized a customer personal identity profile. And it's extensible, and so on.

And some of the categories here are name and address, organization, birth, age, gender, marital status, physical characteristics, language, nationality, visa, occupation, qualifications, passports, religion, ethnicity, telephone, facsimile, cell phone, pager, e-mail account, tax number, spouse, children, parent, home,

hobby, et cetera, et cetera.

So, there are a number of standards organizations working on such profiles that live in somewhat vertical silos. But that's the nature of an identity. It is the sum total of all the information that relates to you. And then any given application may look at, really, hopefully, a minimal subset of this profile for its purposes.

The other thing I included here, too, is because the nature of this panel is identity management. In my way of thinking, identity doesn't exist in a vacuum. I mean, there is no such thing as the sound of one identity clapping, or -- identity falls in the woods, what do you hear kind of thing, right?

Identity exists in a context, and the context that I have described here in one of the charts called identity management is that identity exists in a context of authentication for the purpose of granting access to some service. Identity isn't just for fun, it's not to draw pictures with, and it's not the vaults.

But that's the context I think we're talking about here -- that there is a train of activity, starting with the identity and credential verification and authentication leading to access to certain services.

And in that context, what we're seeing in the

industry -- and by the way, I should have mentioned that an essential element of identity management is an access management system, which includes the user authentication piece, which is the entry point of the entity, or the individual, into the system, or into access to web services, or whatever the value added services are.

It's a critical point, that authentication moment, because everything else bridges off that. That's why I would go back and say that having a strong multi-factor authentication technique tends to strengthen, and will strengthen, the weakest link in the system.

And that's what is so easy and good about smart cards, is I can have biometric plus PIN plus password plus challenge response, PKI-based authentication. I can put them all together, depending on the demands for the strength, and all that can be based off of a smart card.

The other important element of an identity management system that we have talked about here is what is called single sign-on. The hot button in the industry in the web area right now is web services, value added services, not just browsing for information, but putting a demand on a stronger and multi-factual authentication.

Hand-in-hand with that is ease of use and acceptability and utility issues that all can be summarized in single sign-on. That is, the ability to

log on once to the universe of web services, and then somehow have access to multiple services that I am authorized to have access to without signing on again. That's really the hot button that goes hand-in-hand with web services.

And single sign-on can take on multiple flavors. Single sign-on can be highly centralized. That is, there has to be some place where your credentials exist for the purpose of authentication, to grant you access. So they can exist in a very centralized place, and I believe it's fair to say that's the Microsoft Passport model. All the credentials in one centralized location, I log on to that credential server, and then I have access through its activity to multiple web services.

A more federated model is the one propagated by the specifications from the Liberty Alliance.

MS. LEVIN: Don't go too far into that, because we will steal away Brett's --

MR. WILLETT: Oh, good, okay. Suffice it to say that the idea is that multiple identity servers are all federated. I log on once to one of them, and then assertions are passed among them.

Let me propose that there is another boundary condition at the other extreme from totally centralized.

What if all of my credentials could be on this smart card, and when I present this smart card, I log on to the smart card in a trusted environment, and from there on I have access to the web services that are appropriate?

Now, there are technical difficulties with that model in the purest sense of the word, but let's not forego that as part of the -- well, obviously it will be a hybrid system. We will have totally centralized subsystems, we will have federated systems, and we should have this boundary value system, at least as a consideration, when we can, so that I, as a user, control the release of my personal information directly in hand.

MR. PURCELL: Now, Michael, there are a couple of exceptions, I think, to something you said there, and one is the SIM chip model where, if I go to Europe and I purchase a 50 Euro chip for my phone using cash, I can put it into my phone and begin to use that phone, and it authenticates that I have access to a certain number of minutes, but it doesn't necessarily carry any identity.

MR. WILLETT: Well, when I say identity, I should always qualify that as identity or, you know, entity identifier.

MR. PURCELL: Right.

MR. WILLETT: We're talking about an individual, because the technology supports the identity

of any entity, be it single or multiple or group or anonymous.

MR. PURCELL: Right. So it's important to make sure that we understand that in that model, you can essentially authenticate, or identify an account.

MR. WILLETT: Mm-hmm.

MR. PURCELL: And that account is a 50-year-old cell phone account that is depreciating as you use it. But it's impossible to track any further than, probably, where it was purchased.

MR. WILLETT: And that's why I point out -- and I should have pointed out -- that any of these profiles, like customer profile, in any given application -- name, address, and some of these other parameters -- may not be a part of that application.

MR. PURCELL: Right.

MR. WILLETT: It could be that only account information is the required minimal information extracted from the profile.

MR. PURCELL: So, smart cards give an opportunity for the kind of flexibility that was encouraged by both the CDT principles and the NAS study. It doesn't necessarily, though, work in all cases, because, of course, just because somebody is using a certain smart card doesn't mean they are the same person

that that smart card is authenticating or identifying, if they can guess the password that is dual factored to it.

Often times, what we have seen is smart cards in the early days now, with very weak -- they tolerate very weak passwords, because they think that because the smart card is cool, you don't need much of a password. And that's starting to break down a little bit. So passwords are still part of that --

MR. WILLETT: Well, you actually have smart cards now that have the biometric reader directly on the card. Or, you could have a biometric reader attached to the trusted system, and make that part of the loop.

MR. PURCELL: Right.

MR. WILLETT: Which is a much -- it depends on the value of the application that's being supported.

MR. PURCELL: Now, so Michael, we gave you a good segue here to talk about the federated systems, and just the way that -- what happens to the data? We have been talking today quite a bit about SSL and how it encrypts across the pipe, but then whatever happens once it lands, what happens then?

And the question is what's going on on the back end, there?

MR. MICHAELS: Well, you know, I get the opportunity of being somewhat at the end here, and

hearing a couple of different thought processes here. And what strikes me about the world we live in -- and you pointed it out first, Daniel -- is that we are very pregnant with identity management. We have been pregnant with identity management systems for as long as we have been having user accounts on computer applications.

And to say that we now want to have identity management systems is perhaps not the right way to put it. I think we need to potentially relook at all of the existing management systems that we have as an organization, or as an agency, or ones that we interact with as citizens, and try to figure out a way, potentially, to do a better job of identity management.

So, what does that mean, practically? Well, if you look at an organization today that is deploying applications for citizen interaction or business to business interaction, or government to citizen interaction, what have you, typically the individuals who created those applications created their own identity management systems.

And they are completely disparate. There is no centralized approach to how the identities are managed, there is no common storage of those identities. And you will have in any organization, anywhere from one to maybe 3,000 or 4,000 or more. I know some government agencies

who could claim up to 30,000 different ways of managing identities.

So, I think we have an opportunity here, and the opportunity here is to consolidate some of the thought processes of identity management into a lesser number of systems, and to do it on a platform that abides by the principles that are put forward by my colleagues.

The issue is why hasn't that happened? And we have talked about passwords, we have talked about strong authentication. Why doesn't everybody have a smart card? I certainly would like to see it happen, my company being in that business, but I think what we have to some extent is a cultural problem.

And I think we need to understand that the individuals who are developing applications are driven primarily by one thing: their business requirement. And if we can't figure out how to infiltrate these principles into business requirements and make them be of economic and social value to the people who are developing the applications or using the applications, none of this is ever actually going to practically happen.

So, if you look at, for example -- I am sitting around, wondering whether I am going to get my Palm that I ordered from somebody on eBay, who I don't know who the heck it is, right, and I bought it through Western Union,

and read the article in the Washington Post about why you should never do that. So I now have an application where I would really like to know who that individual is, just to the point where I felt if I didn't get my Palm, I have some way of getting back to that individual. And I am relying on a trust identity model within eBay, which is, you know, reasonable.

But as those types of demands grow, I will demand, as a citizen a greater set of identity management, and my service providers will apply techniques, technology techniques, that I think will meet that.

So, I think we can all look into organizations today and see the opportunity to recreate what we have. But fundamentally, just to answer your question, if we don't start to consolidate the identity management systems to drive simplicity and efficiency, I don't think we're ever going to get to the point of being able to deliver on any of these principles.

But we can put the two together, the driving factors of business and the benefits of privacy, and get there if we do.

MS. LEVIN: But can you tell us a little bit -- I know we don't have much time left -- about how a single sign-on system might incorporate the CDT

principles and the NAS recommendations?

MR. MICHAELS: Well, the mechanisms of identity management system can be distilled. And you did a pretty good job, here, I think, of distilling what is an identity management system.

And so, basically, by implementing a common set of technology -- which could come from multiple vendors, it does not have to be a single system -- you can, basically, take all of the authentication mechanisms, and the access control mechanisms that are out there in different applications, and consolidate them to a single function, an infrastructure function.

To some extent we have directories in our organizations today, where you can look up people's names and e-mail, and so forth. That's really what we need to provide, is an infrastructure piece that applies to a service to the different applications. And that's what an identity management system, at the end of the day, does. It provides an infrastructure, a service, to the individual applications that that can be reused, so that you're not recreating the wheel.

Now, if you do that, you have a place where you can deploy policy, a centralized place where you can deploy policy. You can have some way of delegating administration of that, but the point is that the

principles of what type of authentication you're going to have across the enterprise applications or consumer applications, what type of privacy concerns that you're going to implement, in terms of securing the data down to the element level, can be controlled by a common system with a common set of vulnerabilities, so that you can fix the vulnerabilities if you see them, and a common set of policies, which right now is just not there, right?

If you have 200 different mechanisms, you will never be able to implement the overall implications of the policy. So I think it is the enabling mechanism, and it's not purely technological. I mean, just simply consolidating the process would be applicable.

MS. LEVIN: Well, to what extent, though -- we heard all day about the difficulty consumers have in understanding technology and these systems, which can be very complicated, but we realize that consumers need knowledge in order to exercise appropriate controls.

How, in these new systems that are evolving for identity management, will consumers be given knowledge and control?

MR. MICHAELS: Well, I think the number one issue with respect to interacting with consumers and technology is that it has to be simple, require a minimal amount of interaction, but at the same time, give

control.

And we talk about different type of authentication mechanisms like smart cards and tokens and biometrics, and all sorts of things. But at the end of the day, the only things that ever get adopted by consumers, or ever really work for an organization are the things that are simple.

And so, if we can make the process of managing identity simpler, reduce the number of points we have to use to manage what our identities are and what the attributes associated with us are, then we will see much more common uses. It will be a more valuable system for the consumer.

Liberty Alliance, to that point, aims to consolidate the functions of identity management so that a user can create an identity and then reuse that identity amongst different business partners without necessarily having to reveal to each business partner, all of the identity information. It holds absolutely tremendous promise, and it has the benefits of simplicity.

And so, we begin to put this type of technology into our consumer-facing applications, we're going to be enabling quite a few more business interactions that we were unable to implement before with the abiding

principles of privacy.

MS. LEVIN: We see we have a couple of final comments, and then we will see if we have any questions, too.

MR. PURCELL: Ari?

MR. SCHWARTZ: I kind of wanted to add on to what he was saying in terms of -- and it goes into what Danny was saying, as well. We have many types of authentication today, and of identity management systems.

We are seeing it come to single sign-ons, to management all of these, to the smart card. It's becoming more centralized, which creates the privacy concern, but it also creates this moment of opportunity to refocus privacy in these systems that, today, really don't work that well.

And security, as well, though our principles don't talk about security. But I think that this is the time when, as these systems do merge into one place, or to a fewer number of places, that we have to address this, or we're going to end up with a system that really doesn't work, instead of one that is simply flawed, as we have today.

MR. MICHAELS: And I would argue that the most important thing we can do is to not start the conversation with technology, because if you get into a

discussion of how PKI could be a benefit -- it will be a benefit, and so will smart cards, and so will user names and passwords.

But if we can start culturally on how to embed the need to enable consumers to be able to interact more with whatever system you have, and also by privacy issues, to control your own risk, in terms of managing other people's information and their identities, and then back our way into a technology solution, I think we will be in much better shape than if we go the other way around.

MR. PURCELL: Okay. Danny, I promised you first, then Michael, then we have a question.

MR. WEITZNER: Thanks. I want to be clear that I am speaking only on my own behalf, not on behalf of my colleagues on the committee, or on behalf of W3C. And the reason I am saying that is because of what I want to say.

I think that there is no question that this is a hard set of questions, and I think it's even hard to know what the questions are, much less answer them.

I have to say that my own personal impression of the state of technology development here is such that I think when regulators, particularly in the consumer arena, are looking to these technologies to provide

anything in the way of identity assurance, anything like that, I think it's important to figure out how to look very carefully and cautiously.

That's not to say that there won't be progress here. I think that the work going on, both in Liberty and Passport is very valuable. I think that there may be a resurgence of some anonymizing technologies, which is interesting. I think there is a whole lot in the offing. But I think to say that we're at early stages is to understate.

And you know, a lot of us participated in some of the early FTC hearings on general Internet consumer issues back in 1996, 1997, and if you could remember the level of fuzziness -- to which I certainly contributed -- at the time, I think we should consider ourselves at that point, if not 10 years before, when it comes to identity management systems.

That's not to say we shouldn't work on them, try hard on them, but I think that we are at very early stages. And I would say that, just in particular to Brett, I think that institutional-based systems, the sort of directory systems you're talking about, clearly are way, way ahead.

And large institutions, as we discussed earlier, have a whole lot more perspective on how to

handle these questions, and I think vendors have a whole lot more perspective on how to market to those institutions, and how to build systems for them. When it comes to generalized consumer applications, this is very hard stuff.

MR. PURCELL: Right. Michael, quickly, please.

MR. WILLETT: I will just continue on the analogy that Brett brought up that at the end of the day. I think the more important moment is about an hour after that, when it's totally dark, and from the point of view that we will never educate -- I don't think education will be the solution to the problem, because we will never educate the masses to the level of granularity that some would like, in terms of technology.

The old saying goes, I guess, we can't leave any child behind. The idea is that a company, the business community, will have to base its reputation, its livelihood, its existence, on the trustworthiness of these systems. I mean, we trust our banks, most of us do. We don't know one whit about how it works, but we have built up over time a trust.

Trust is not a technology, it's a sensation we generate in a customer. And that sensation is idiomatic, it's very hard to generate and to sustain. But businesses have to stake their reputations -- and I think

they're doing that in the web services arena -- on the trustworthiness and the dependability of these systems, and suppress the technology, make it all transparent.

People don't want to have technology explained to them, because -- what I find is that people get very nervous, the more they understand about certain technologies. So, again, education has its purpose, but I think it can't be guided to the nuances and the details of the technology. It has to be at a different level.

MR. MICHAELS: I would just make one point. I would just give an example of something I was thinking about while you were talking in terms of trust.

About two years ago, three years ago or so, I went into my -- well, I won't name the investment company -- but I went into this online investment account that I have, and I was looking in there, and I noticed I had $2 million extra dollars in my account, literally.

PARTICIPANT: What are you doing, sitting here?

(Laughter.)

MR. MICHAELS: Well, I didn't put it there myself, so I was a little concerned that this appeared in my account. So I called up the offices of the company and said, "Look, there are a lot of stocks here that I didn't buy, and I'm kind of wondering what happened here."

It took them about 20 minutes for them to believe me, right, because that doesn't happen every day. And then they, over the course of seven days, took out all of the transactions, moved them over to the right individual who lost the $2 million, and fixed the problem.

And so, obviously, I was concerned, lost a little faith in the organization, but I was the benefactor of $2 million, so I really wasn't in trouble -- at least I didn't spend any of the money.

So, had it gone the other way, had I been the individual that lost the $2 million, first of all, I would have lost a lot of trust in the organization, and if this was not a recoverable event, if this organization stood up and said, "Listen, you transferred this stock to this other account, and sorry, you're out of luck." And then, "You signed in, you logged in, you put your user name and your password in there and transferred it out, and I'm sorry, at the end of the day you don't have $2 million any more," and you sit there, "Oh, my God, I just experienced an identity theft," but this is a very simple identity theft, it's just a user name and a password. At that point I would have been thinking, "I think we need a better model here," right?

And it's types of things like that that will

continue to occur, or people thinking about how to prevent them that I think will drive us to do a better job in controlling both privacy and security.

MR. PURCELL: Good.

MS. LEVIN: Good example.

MR. PURCELL: Questions? Stephanie Perrin, could you identify yourself, please?

(Laughter.)

MR. PURCELL: Can I have your account number?

MS. PERRIN: I wanted to raise a couple of things --

MS. LEVIN: Flip the mic on, Stephanie.

MS. PERRIN: I think it may be off, unless the battery ran down again. You can turn it on for me, I've got my limitations.

Definitions. I think Lynette started this by saying definitions were important, and I notice throughout the discussion that Michael was very careful to go back to the concept of entities and authenticating entities, and using that with smart cards.

But generally speaking, these two processes that went on, the Academy of Sciences and the authentication principles working group that Ari was talking about, focused on identity. Is that right? Or, authentication?

My point being if Dr. Roger Clark were here, he would be grabbing the microphone and going, "You can authenticate entities, you can authenticate goods, you can authenticate transactions. You don't need to authenticate identity."

MR. WEITZNER: I think we say that.

PARTICIPANT: Nobody knows you're a dog, right?

MR. WEITZNER: And Roger came and told us to make sure we would say --

MR. SCHWARTZ: And even beyond that, taking off from the NAS report, we distinguish between individual identity versus non-individual identity, device identity, et cetera, and attribute authentication, which may have nothing to do with an individual, or may be tied in some way towards identity.

MS. PERRIN: But attributes, in the definitions, are linked to individuals. And I guess that's what gets me with my Roger hat on here, is how do you peel -- and it's not easy -- how do you peel these things off and talk in the abstract, where you're really only authenticating a right, a service, a value, as opposed to an individual.

I think, to get back to what Ruchika was saying, you really have to start from scratch. And we can start from scratch, but it's so easy to fall into

that well-worn rut of where we are now.

The 145 passwords and log-ons, that's a product of the fact that there was no monetary value in the beginning of the Internet, and the New York Times and everybody, in order to use their free service that was costing you money, they at least collected your name and your personal information, or "Mickey Mouse" 463,000 times.

But that's a rut, it seems to me. We don't need that kind of log-in authentication to --

MR. SCHWARTZ: But there is the idea in the NAS report about an authenticator, though, which is not an identifier.

MS. MILLETT: Right.

MR. SCHWARTZ: Which is a -- go ahead.

MS. MILLETT: So we -- the committee was originally charged to look at user authentication and privacy -- privacy of people, not privacy of objects. So that was our original focus.

We moved beyond that, and in fact, we have a fairly abstract definition of authentication, which I probably won't get word for word, but it's basically -- the process of establishing confidence in the truth of some claim.

So, at that level, we -- and I actually wanted

to make this point earlier -- we are not claiming that our definitions are the best, but we had a group of pretty smart people's blood, sweat, and tears at some points. We hope that it helps to move the debate forward a little bit, and abstracts enough that maybe we can move further.

But the original charge was about --

MR. SCHWARTZ: We actually originally used Roger Clark's definitions. And actually, we found it easier to have the discussion about some of the nuances with the NAS definitions. People wanted to change Roger's definitions, so we went with the NAS.

While Roger's are a good starting point, I think, in the way to think about, when we got down to the practical nitty gritty the NAS definitions, were easier to use for us.

MS. PERRIN: Good. Thanks. I would just like to throw in that -- and Danny went back to it later -- I did not want to leave the impression this morning that we had done privacy-enhancing technologies and anonymity tools and tried that, been there, didn't work.

I just think we were about 15 years ahead of the time. And the question now is how are you guys going to set up market drivers to make privacy-enhancing technologies actually get some investment, and some

deployment?

MS. LEVIN: My sense is that we're going to be spending future time at the FTC looking at these issues with a lot more care than we're going to have time to do today, because it certainly will warrant that attention.

So, we will come back to those very important questions, but Richard, go ahead with one more.

MR. SMITH: Yes, hi, Richard Smith. The question I have is I don't feel like, when I'm on the Web, I have much of an identity management problem, that I don't see why I need a single sign-on, or anything like this.

But what I would much rather have is when I go to a website and I want to buy something, particularly in a place where I don't really have a need for an ongoing relationship, I just want to buy something, why can't I just take my little credit card icon that's on top of the screen and drop it on the order form, and I'm done?

And what I feel like is maybe identity management systems are trying to give that to me, but all I really want to do is be able to buy stuff on the Web with the same ease that I buy it in the real world.

But everybody seems to want to do this centralized thing, and I would much rather have my data -- to have my computer, and just make it easy for me to

buy things, because I find myself now skipping over and not going with websites who insist on me setting up an account in order just to buy something really simple. And I would just like to hear the comments on that.

MR. PURCELL: Personally, I agree. I think that it would be fantastic, and I think part of the vision that some companies that are pursuing is this issue of having attributes that are not connected to your identity.

And an attribute could easily be a payment attribute. A credit card company could give you a credential that essentially says, "This person is good for it," you know, "up to $500," or something like that. And if that were what then freed up the shipping of whatever product you're buying, what would happen is the vendor would not have your credit card information. They would simply have a credential that they submit to the Visa system that essentially says, "Hey, you gave me this funny number that's all encrypted and everything, and you said this person was good for it, so give me my $59.75 that this person has charged against this."

And we believe that those kinds of attribute authentication processes are possible, following these principles, and that some companies are actually working on those.

Just like I'm over 6 foot, or I'm over 21, or I -- you know where I live, just have that person ship the stuff to me, but don't tell them where I live. UPS is an example. They could say, "Yes, just put this bar code on it." UPS will know how to deliver that, but the vendor doesn't need to know.

MR. SMITH: Well, a lot of that is around -- it's fairly complicated, in terms of infrastructure, what we have to do. And I'm thinking of something relatively simple, which is I have to keep typing this stuff in over and over again, so even with today's infrastructure, I would be more inclined to do online shopping -- if services thought more in terms of the client's eyes, as opposed to service's eyes --

MS. LEVIN: Okay, I --

MR. PURCELL: Well, I think that's funny. I mean, one of the things that I keep hearing is that, oh, it's not roamable. Well, that shouldn't stop people from -- you know, if it's device-centric, then it's not roamable. You can't necessarily take it with you. Big deal. If you want something that's device-centric, you ought to be able to get it.

MR. MICHAELS: Looking at Liberty Alliance there has been quite a bit of work there. And if you were to implement all of the concepts of Liberty

Alliance, it would be pretty technologically intrusive.

But when you distill it down to the idea of adding some of the Liberty Alliance identity concepts into your environment it really isn't that hard, from a technological point of view, and you can pick up a simple identity with a simple number of attributes, like your name and your address information, which is essentially, I think, what you're looking for, plus some credit card information.

You could do that with a bank, and it's not much technology to take the attribute acceptance, if you will, and integrate that into Web application and bring that up fairly quickly.

And I think we're going to see that, actually, over the next 12 months. Folks are going to get digital identities from identity providers, like banks, who really want to do this, and they are going to hold that basic information for you, on your behalf. It will go with you and you will basically transfer that information to whoever you feel like you need to, via the Liberty mechanisms.

It's going to be very simple, and I think you will see a wholesale change. And it's built on the idea that there is no centralized mechanism of storage of all of those attributes, and so forth, so –

MS. LEVIN: We're going to have to stop at this point. I am not a fortune teller, but my crystal ball tells me that we are going to be spending a lot of time in the next couple of years looking at these issues, and so I promise we will revisit them.

We ask now -- we're just going to take basically five minutes. Stretch, get something to drink, come back, because we have a terrific last panel of the day, and I don't want to cut it short.

Thank you to this panel, it was terrific.

(Applause.)

(A brief recess was taken.)

MS. LEVIN: The mics are on. That means we're ready to start the last panel. If everyone would please take your seats.

PANEL 5: BUILDING SECURITY INTO THE ARCHITECTURE FOR SAFER COMPUTING

MS. GARRISON: Good afternoon. Again, I am Loretta Garrison. I will be moderating today. Welcome to the final panel of day one. It has been a really exciting, stimulating, challenging day for all of us, and we appreciate your continuing to hang in there with us. We realize that we have a very full agenda.

I would like to introduce the panelists for this last session. From my left, the far end, Alan Paller. Next to him, Jim Halpert. Then Gerard Lewis, Andrew Patrick, and to my right, Frank Reeder, Phil Reitinger, and Howard Schmidt. Also joining me is Toby Levin, from the Federal Trade Commission, to assist.

We have gained much insight and understanding today about what has happened to the technologies that protect consumer information, and why they have and have not worked, what it is about consumer behavior that makes technology-effective, and what is actually used by consumers it's designed for, and about building protections into the architecture of identity management systems.

Picking up on a design challenge that we heard from this afternoon's opening panel, we are concluding this day with a discussion about building security into

the architecture for safer computing.

To begin with, we will have introductory remarks by Howard Schmidt, who is going to give us a report card on the current status of the security of home computing. Howard? MR. SCHMIDT: Thank you very much, Loretta, and thank you all for being here and giving me the opportunity to talk.

I would be tremendously remiss, had I not started out by thanking Loretta and Toby for the work that they have done on pulling this together. I know the term herding cats means absolutely nothing when it comes to the work that they have done, but I very much appreciate it.

MS. LEVIN: James Silver, as well. We're a trio.

MR. SCHMIDT: Oh, okay, great. Thank you.

MS. GARRISON: Thank you.

MR. SCHMIDT: Anyway, I want to just quickly talk a little bit about the report card of where we have been, where we are, and, presumably, where we are going, relative to consumer online security.

And I want to do it by framing it, first, from a perspective that it's not just the technology. You know, we have this other PPT that we talk about. It's the people, the processes, and the technology. And so in

looking at that, we look at a broad spectrum, what it means to be safe online, what it means to have a safe online experience, and how computing is safer now than it has been.

Then I want to break it down into four specific areas, and it's particularly rewarding to follow the previous panel that discussed so much the areas around authentication and public infrastructure, and the need for revamping this, and how it relates to the things we are doing. Because one of the first things we need to look at is where we are today, where we have been, as a report card, regarding authentication mechanisms.

It seems that much of the world today is framed in pre-9/11 2001 and post-9/11. But I actually want to roll back a little bit further to pre-2001, and I use January of 2001 as sort of the linchpin, because prior to that, we didn't have that culture of security that Orson and many of us have talked about. We've started to move a lot closer to that.

So, if you look at that authentication piece prior to January of 2001, it was pretty much anybody's guess out there. There were no requirements, no recommendations about strong authentication mechanisms. In many cases, the software that came installed had accounts on there that were administrative accounts that

required no passwords and no one even knew that.

Then we zoom ahead to the 2001 to 2003 time frame, where we basically -- every time a window opens up on one of the online services, it says, "Do not give out your password."

There are windows that come up that are basically just for the authentication piece. There is an encrypted session that takes place between your computer system and an authentication computer that makes that a safer experience, so someone can't grab the data as it transits itself and pull passwords out of there, which used to be the older way of doing it, prior to 2001.

We see an increase of use of IPSec and SSL and these sorts of encryption technologies. We also see better protection of privacy, as part of that consumer experience, post-2001.

And I want to zoom into now the future piece, and that's where are we going with the authentication piece from our report card, and that's the fact that strong passwords are now becoming very commonplace.

The downside is it's very difficult to remember, which is why the next piece of this, which we are starting to move to, is the two-factor authentication, whether it's smart cards, biometrics, whatever mechanism one would use, we're starting to see

that becoming more and more relevant. We're starting to see a lot of discussion and a lot of the building of that into the consumer space, including the operating systems which now support that.

We have also seen an increase in the number of reportings, which, once again, makes things safer. If you look at the neighborhood watch type concept, where you have neighbors looking out for neighbors, other people putting up signs saying, "Listen, if you see something suspicious, notify someone."

We actually now are training state and local law enforcement. We are getting a tremendous amount of support from the FTC working with the consumer, and understanding how do you report these things, where do you wind up sending information where your experience has been less than positive, for malicious activity? So that's sort of the authentication piece.

The next piece I want to go to is the configuration, and this is very crucial. Prior to 2001, most of the systems were designed for usability and manageability, especially in the consumer space, especially for the desktop person. It was, "How easy can we make this?"

Unfortunately, the easiness also gave us a very wide window to make it less safe, more accessible -- for

bad people to do bad things to the system, including just some of the basic, core software running on your system that you didn't know was running on there.

You know, we have seen a number of cases where viruses and Trojans, and some of the things that have occurred that have either pulled password files down off of people's systems, opened those -- installed Trojans, where people could then take over a consumer's system. They were able to be successful because there were underlying components that were running that people didn't know about.

In the 2001 to 2003 time frame we have seen that change dramatically. We have seen a mixed bag of changes that have taken place, normally through the process of doing updates, normally through the process of telling people, "Here is a patch, here is something you need to do to make your system more secure," that either turns off those services or reduces the accessibility from the outside world of those services.

Then, of course, the current state, and once again, increasingly so in the future, is the whole concept of secure out-of-the-box. When you log in on the system, whenever you first turn on your system and plug it into your cable modem, you won't have blank passwords on the system that someone could automatically take over.

You won't have services running on the system that someone can then compromise and work there.

And the same thing goes with access points for wireless. Cable modems, DSL, and wireless technology are phenomenal. I have been using it since I could get my first cable and load them up on the mountain. I have been using wireless since it first came out. And what we're seeing now is that transition over the past two years, where the wireless manufacturers, the cable manufacturers are putting personal firewalls into the hardware, in addition to software-based things you are running.

You are also seeing upgrades that they have on their systems for those of us that have older systems, where basically you can go into the system configuration on the wireless access point, and it says, "Download your free personal firewall, download your free anti-virus software." Those things are there now to better protect the consumer, to make our online experience much better.

The third piece of this is the awareness. Prior to 2001, it was word of mouth. If we knew somebody that had something bad happen to them, you would generally hear about it, but you didn't see much publicity about it. You saw instances where SANS and organizations like that would publish information,

generally to the IT professional community, but the consumer side generally didn't subscribe to those sort of things.

So, in the 2001 to 2003 time frame, we have seen SANS, vendors, the information sharing analysis centers, the ISACs, media, FTC through the Dewey site and the information security site, the White House, working with the Cyber Security Alliance to put up websites, FAQs, how to help consumers better enjoy the experience, while protecting themselves.

And of course, moving forward, what we will see taking place are situations where customer service will have security and privacy as part of the core competency. When you call in to someone about why something doesn't work, there will be the discussion about security and privacy. "Do you have this enabled? Do you use a strong password?" These are things that are going to be part of the core DNA, as we're moving forward.

And including the ability to provide services for the websites. One of the things I have seen recently, particularly on the broadband deployments, where when you log into the website at whatever cable carrier it is, just like they do on the modems, they have a link that says, "Click here for security, click here for privacy." So these are things that we're seeing in

the awareness piece.

And lastly, and the one that I think eventually we will be able to say, "Gee, that used to be a problem back in the early 2000s," and that is that whole concept of patch management.

Whether it's Linux, Windows, OS10, Sun, Oracle, we have seen in the past it was sort of a pull. If I knew there was something that I had to fix, I would go out and pull the bits down and fix it. I would pull the data down and fix my systems. And the 2001 to 2003 time frame, we saw this service where you can sign up for it, where it will say, "You need to fix something on your system. Here is the data that you need to do that, here is the link to do that."

And you have some options. Currently, in most of the situations, they will automatically install it for you. In many of the operating systems and many of the major applications, for the consumer space, the same thing.

You have a box. If you're technically competent, like some of us may be, we may want to say, "Well, tell me what it is before you install it." Other cases, "Please do it, because I don't want to have to worry about it." I use that 86-year-old father of mine as the example of, "Please do it, I don't know what I'm

doing. Fix it for me."

And then, in the future, of course, it will all be push. We will have the self-healing, the self-repairing systems. We no longer will need to worry about having a bachelor's degree in computer science in order to have a full and safe consumer experience.

So, in closing my opening comments, I want to cite something that I attribute to Doris, and a lot of the work around the OECD, and that's my definition of the culture of security in the online world. And the analogy I use is the seat belt example that some of you may have heard before.

You remember back when seat belts first came out? We found out a couple of things about them. First and foremost, they were extremely uncomfortable, because when we sat on them they hurt after a while. But that's what we did, we sat on them. And despite the best efforts of the highway transportation folks, despite the best efforts of law enforcement, we sat on the seat belts.

Then, later on, they put those annoying buzzers in there, and we learned that they become even more uncomfortable when you get them a little bit higher behind your back, because we would connect them behind our back to shut off the buzzer.

And then, eventually, it got to the point where it became part of the infrastructure, part of the car. And I remember the first time I sat in the car, closed the door and this belt automatically goes across me, and I think, "If you're going to go to that much trouble, I'm going to wear it."

Then I ask any of you today, as I have said many times, find a six to eight-year-old child, put them in a car, and what's the first thing they do? They buckle that seat belt. That's the culture of security that we have seen in that world. In some instances, it took regulation, and in many, many instances, it was done because it was the right thing to do.

And that's the same thing as I see us moving into the consumer space as I look at our report card two years from now, in saying we will have that culture of security. These things will be built in from the very beginning. We will have a user base that is much safer, respectful of privacy, and has a much richer online experience as we move forward.

So, thank you very much for the opportunity to give those opening remarks.

(Applause.)

MS. GARRISON: Thank you, Howard, and we do look forward to that report card in two years.

We have heard an awful lot today about people who are struggling in many different ways in trying to use their technology. The 144 passwords certainly stands out.

But the big message that we also heard from the consumer groups and from the academics, is that it has to be usable, it has to be simple. It has to be integrated into the system, you just turn it on and it works. And it has to be interoperable.

So, part of the challenge here today is how do we talk about designing technology for safer computing that incorporates these features?

But before we get there, I would like to ask first, is home computing safer today than it was a year ago? Why, or why not? Jim, can you help us with that?

MR. HALPERT: Loretta, I think it is. And Howard outlined a number of very important ways in which things have gotten better, if one takes 9/11/2001 as the measuring point.

There is greater awareness among consumers -- and we're focusing here on the consumer market -- and on the providers of various technologies, and providers of Internet service.

I am here as general counsel of a trade group of leading ISPs called the Internet Commerce Coalition,

and I can tell you that all of these companies invest very heavily in upgrading network infrastructure, increasingly in R&D, actually, to develop network security solutions. They are working actively on rapid and coordinated and collective responses to security threats in the network, like denial of service attacks and worms.

And in many cases, companies will discover problems and alert their competitors, because this is a common issue of trust in the network, and something that network operators are uniquely situated to address.

They are also investing in detecting and filtering out the transmission of malicious codes, such as e-mail viruses, worms, Trojan horses, and denial of service attacks. These are automated mechanisms to try to stop these transmissions. They are not always successful. The back-up is to have a very rapid and coordinated reporting mechanism, so that Internet companies can alert each other to problems that are coming down the pike, and alert their customers.

There also is a significant effort to educate customers regarding the importance of network security. This is something that the government can play a very important role in, and the press can play an important role in.

Howard mentioned going to websites and being able to download security tools. Our member companies are investing in robust and prominent security portions of their websites that educate consumers about what to do and not to do with regard to network security, and give them easy access, through clicking on hyperlinks to additional tools to upgrade security.

Finally, there actually is an important role in providing customers with ready access, at the edge of the network, to tools that come with the sign-up for service.

For example, customers of broadband networks can get, through our broadband members, discounted firewalls, in some cases free firewall technology, free anti-virus software with upgrades provided, say, for a year on a free basis, some password protection tools to make sure that customers use secure passwords and have encrypted connections as they log into the network.

And also -- and this is very important on the theme that the FTC has spent a lot of time on in the past -- parental control software, to protect other aspects of security for children, for example, who are on the Internet.

ISPs are much better situated to protect the security of their actual network, rather than the activities or software on end user computers that are

just off the network. However, even there, our members have made major efforts appropriate to the particular market they serve. And this will vary widely.

For example, a big backbone provider that provides a direct Internet connection to a corporate network is going to provide a very different set of security tools to network administrators than will a narrow band provider that is serving consumers in the home.

In addition, proprietary online service providers, like our member AOL, have a different -- and in some ways, an easier job protecting security than providers that are simply entirely open to the Internet.

So, there are a range of different tools, but companies are spending a lot of time and effort on this increasingly important area of providing a good and safe network.

MS. GARRISON: All right, thank you. Jerry, can you give us a summary from Comcast's point of view?

MR. LEWIS: Sure, thank you. And, first of all, thanks to Commissioner Swindle and the FTC for having us. We appreciate the chance to be here. And to the staff, who has done a great job organizing this.

Let me give just a little bit of background. Part of our panel topic today is network architecture,

and I would just like to spend a second talking about where we are in the history of network architecture, particularly with respect to cable-based Internet service providers.

You may remember almost 18 months ago Excite@home filed for bankruptcy. They were the outsourced Internet service provider for many cable operators, Comcast included. And that forced us and the other cable companies that used Excite@home as their ISP solution to scramble quickly, and at great cost, to deploy and build our own networks so that we could, in effect, keep the lights on for our Excite@home customers.

And we, like the several other cable ISPs, did that in about 90 days, literally, logically and physically deployed an ISP network that we had planned to deploy in about 9 months. It wasn't without some fits and starts, but it basically worked, and it's been humming along very nicely ever since.

So, we at Comcast, and I think many other cable ISPs – are at a fairly early stage in the architecture of the network, and as a result, many of our decisions with respect to customer-facing security, I think, have been driven more practically and tactically, given where we are.

And so, what we have decided to do -- at least

currently, at Comcast – is offer a McAfee and -- I'm not necessarily promoting them, it's just that they're the partner we're working with currently -- firewall, client software. It's their standard retail offering that our customers can download directly through our website for free. And it's a one-year free firewall.

McAfee actually owns the customer, provides all the technical support, the updates automatically, and handles the customer relationship, because they're best suited to do that. We don't necessarily have a lot of expertise or depth yet at 1-800-COMCAST for dealing with firewall questions, for example.

That's a model that has worked fairly well. We have had a relatively high adoption rate among our subscribers for the firewall. And when we look at this relationship and other things that we can add to it, we certainly will look at adding anti-virus and privacy, and other types of security tools into the mix. It's really dictated by business considerations, in large part, and by our desire to provide a valuable solution to our customers, who do communicate with us and say privacy is of concern to them, security is of concern to them.

And right now, I think where we are, as many other cable ISPs may be, is that this is a best outsourced solution right now. That may not always be

the case. And over time, our security solution may be a hybrid of outsourced technologies like a McAfee, as well as some home grown things.

MS. GARRISON: Jerry, one question.

MR. LEWIS: Sure.

MS. GARRISON: When did this go into effect for your customers, and what is the adoption rate? Do you have that figure?

MR. LEWIS: We haven't publicized the adoption rate, but in the areas that we have heavily promoted it, it has been very high, and we have been very pleased with the adoption rate. And we are in the process, as we all know, of merging our AT&T broadband systems into Comcast systems that will be complete this summer.

And at that point, we will have over 4 million ISP subscribers, and we will be looking to make sure everybody has the opportunity to upgrade and get the benefit of the firewall solution.

We started offering the firewall, if I remember correctly, about six months ago. Prior to that, we had offered anti-virus services through McAfee. And the way the affiliate relationship works is that people who take the firewall for free can get a special deal from McAfee on the security and the privacy components, as well as their security threat assessment center, which is

actually a pretty cool little thing if you have played with it.

When the deal comes for reupping, we will certainly look at adding new things into the mix, and new values for customers, and give them perhaps a mix of free and discount, so that they can continue to get the benefit of the services.

What we have done in terms of customer notification and education -- and that's really where I think we and a lot of the ISPs, not just cable-based, are really at the early stages -- is developing home-grown materials, FAQs and other education, as well as leveraging what third parties have done.

We're linking to Dewey the Turtle, when the new portal rolls out in about 60 days. There are a lot of other good third-party sources out there that we direct our customers to, so we will continue to grow and enhance that area.

And the user education piece, I think, is very important. It's something that I think we have a responsibility to do, and we take seriously, and are doing that.

In terms of the future direction, the architecture, if you will, of network security, what things might be coming down the road? A couple of things

to speculate about.

I think Jim alluded to it, there will be things beyond pure security that will be of value and interest to our customers. Parental controls is one example. Pop-up blocking, spyware filters, there is an awful lot of things out there that many ISPs currently address that we may address as part of an overall security solution.

You may not think of pop-ups necessarily as a security issue, or parental controls as a security issue, but they all start to get into the overall category of user control over their Internet experience. So, that may well be something that we look at next.

Anti-virus is something that's critical, that we promote heavily. Anti-virus licensing, however, is not always the easiest or most cost effective thing for ISPs to do. So I think for the time being, anti-virus is probably something that will be deployed on a client basis to individual customers, as opposed to on an enterprise basis, where the ISP might do the vast majority of the anti-virus filtering, though we do do some at the network level.

And the last point I will make is with respect to where these solutions go, the privacy and security solutions. Right now, we are following a client model which puts the obligation on the customer to download

software and install it properly on their hard disk. With good tools and wizards, that can be a relatively painless process.

But again, that's work. And as I think we have all heard today, and I think we're all in agreement, the more work for people, the less likely people are to use it. So we want to simplify that.

We have looked at, and will continue to look at deploying security and privacy technologies on our network at our end. There are different issues and considerations there.

If we were to deploy a security tool that four million or five million ISP customers had to access, that's a whole different calculation for us. Different hardware requirements, scalability requirements, that we don't necessarily see if we push the solution down to the customer. So that's part of the cost benefit analysis that we constantly do.

And there may be other extended factors that impact security on the network. They may be external factors. For example, law enforcement requests or requirements on the telecommunication side. The Communications Assistance for Law Enforcement Act (CALEA) Statute sets fairly strict technical requirements on the telephone network for intercepts, and the like. Perhaps

there will be some counterpart or equivalent on IP-based networks at some point in the future.

So, there may be a variety of external constraints or guidelines, legal or standards, or otherwise, that are impacted. But that's, in a nutshell, what we have been doing. I would be happy to answer any questions later.

MS. GARRISON: Thank you very much. Phil, can we hear about Microsoft?

MR. REITINGER: Sure, Loretta. Thank you. But I'm not going to talk just about Microsoft. I also would like to compliment the FTC for separating Alan and me at far ends of the table to prevent me from needing a transfusion by the end. But it was unnecessary.

MS. LEVIN: Not deliberate.

MR. REITINGER: I will take Alan's criticisms with good grace, and thank him for his compliments for the things he thinks Microsoft has done right.

Let me answer the question as directly as I can. Is computing safer now than it was several years ago? The answer to that is yes, but I think it's a complex answer.

First, statistically, I don't think we know. In other words, we don't have good statistical metrics for how secure the Internet is, and we don't know,

statistically yet, how prevalent cyber crime is. There is a lot of good work that has been done, including by groups like the FBI and CSI out in San Francisco. But a lot of that is anecdotal. So we don't have good measurements yet to know how good a job we're doing.

However, we do know that software has become more secure, for a lot of the reasons that Howard identified, and Alan identified, also, earlier.

The old paradigm of functionality over security has changed. It no longer is prevalent, I think, in the industry, both for Microsoft and for other software players. And I think there are a lot of reasons for that.

September 11th is part of the reason. I think we see a greater market focus on security every year. All you have to do is attend the RSA trade shows, and watch the number and quality of security products that are available.

And I also think the industry is maturing. And as the industry matures, it's doing a better and better job of addressing the spectrum of issues that it needs to.

So, you see things like -- and I will use Microsoft terminology here, because it's what I am most familiar with, I work for Microsoft -- the creation of

the trustworthy computing initiative January 2002, which has 4 distinct elements: security, privacy, business integrity, and reliability. So, security and privacy are both in that, and let me drill down a little on security.

Howard, I think, has already covered most of the major elements of that, but it's not something that's relatively simple. There are four elements in Microsoft's terminology.

"Secure by design." And this gets to the specific topic of the panel. It has two features, essentially. One, writing better code, not putting vulnerabilities in. And secondarily, architecting for security. As you go forward, designing products so that, for example, processes run at the lowest level of privilege possible, if we can get to some level of technical specificity there, dealing with some of the issues that Alan raised earlier.

Second, as Howard was talking about configuration, "secure by default." Products that are secure out of the box, both server products like Windows 2003 that Alan talked about earlier, and consumer products, so that products like Outlook, from Microsoft, now ship with much more secure default settings.

And then critically, as we move to unmanaged environments, "secure by deployment." Making, as Howard

said, patching easier so it's automatic, it can be done as transparently as possible to the consumer, and providing guidance on how to configure systems securely. Microsoft has done configuration guides, and we have been assisted by other configuration guides, such as those done by CIS and Frank Reeder, on my right.

And finally, "communications." Providing a rapid response capability that's also associated with secure by deployment, and communicating with people about what we're doing, such as through the MSRC, the security response center at Microsoft.

Now, what does all this mean? Does it mean that we're not going to see vulnerabilities in the future? No. I would like to harken back to where Commissioner Swindle started us. And if I could paraphrase you for a second, sir, we're not going to find a solution, but we're going to solve a lot of problems as we work towards that end. That's exactly right.

We need to make computing reasonably secure, so that it's functional and that we address the problems, both as they come up, and proactively, before they come up. So that's the second point.

The third point, yes, software is more secure. But it is also true, as we learned this morning, that the threat is increasing. Hackers are really, really good at

developing new attack technologies. And they are a lot better at sharing information than we tend to be in the private or the public sectors.

So, industry needs to continue to innovate, and continue to develop more and better security solutions and architect products better. Because we've got, essentially, two growth curves, increasing security of products and increasing threat. We have got to make sure that we widen the gap so that security increases, rather than decreases, over time.

And the fourth point, and then I will close, is technical solutions are not sufficient, in and of themselves. As Howard had emphasized, we really need a multi-disciplinary response, more secure technical infrastructure, management solutions, education, R&D, deterrents so that when cyber crime happens, we put the bad guys in jail.

So, when the question is put what do we need to do to address computer security, the answer is D, all of the above. And you can write whatever you want there, it's all of the above. Thank you.

MS. GARRISON: Thank you. Phil and Jim have both said that home computing is much safer today. But Andrew, can you quickly recap what consumers think about safer computing?

MR. PATRICK: Great, thank you. Yes, I want to buck the trend and say computing, from a home user/consumer point of view, is a much scarier place than it's ever been.

When you think about users' concerns in terms of the major things they are concerned about, their security, their information security, their information privacy, their experiences when going online and threats to their system, it's a very scary place.

Consider, for example, a scenario where you're asked to go and help a couple with children go and buy their first computer at a computer store, and you've been asked to tag along, because they think you know something about computers.

So, you go and pick out a reasonable computer configuration for a home computer, and you might pick up an office suite, because they want to do some word processing, and they want to go on the Internet.

You can't stop there. We have talked about at least eight different things that you also must buy at that computer store in order to be running something that is reasonably secure, safe, and will have good experiences. Anti-virus software, anti-spyware software, cookie management systems you either have to buy or learn how to use, things like P3P and cookie washers.

Firewall, perhaps two of them, hardware and software. A pop-up blocker, because that has a lot to do with experiences, especially experiences with children and what they see, and what you might not want them to see.

Some kind of a spam control system, and some kind of a parental control system. That's a lot of stuff to buy and to configure and use. My quick calculation on the back of an envelope says it probably adds about 15 percent to the cost of the system before you've been out the door, which is not insignificant.

All of this is for something that you don't want to do. You didn't buy the computer to do this. You bought the computer to do some office applications, to write some good-looking letters and reports, and to help the kids with the homework, and go on the Internet.

So, the other big problem is none of this is your primary task. Your primary task is not to operate a safe computer. Your primary task is to do the things that you want to do. So, we have problems that are not related to why people are using computers, and that makes it very hard for people.

MS. GARRISON: Thanks. Howard, I would like to talk about barriers to safer computing. For example, lack of education, technology, money, will, and also

about legacy systems. Are older computers a risk for security, for personal use?

MR. SCHMIDT: Yes, I think I will start with the last question first, and address that, because that, indeed, is one of the issues we have looked at for a long time.

If you envision the IT space today in three boxes, there is the legacy systems, there is the world we're living in now, and the future systems. The future is one I think we are all very, very convinced that things will be more secure. They continuously work better, as Phil pointed out, as have a few of the other speakers.

The space we're living in today is we're enjoying the experience, while we're fighting some of the Trojans and the viruses and some of those things. But all in all, it's a positive experience for many people.

But the legacy piece -- that's the part that creates a lot of the problems for us. In some cases, the software was not designed to be in such a threat-ridden environment as you know, "always on" connections provided us. The software is, often times, not as robust in looking for viruses and blocking malicious codes, and things of that nature.

So, consequently, I think the easy answer is

for just everybody to upgrade to the latest product, which is more secure, more privacy aware, but unfortunately, there are some financial constraints in conjunction with that.

So, I think that's the biggest barrier I see right now for being more secure quickly, it's just some of the legacy systems or products that's out there.

MS. GARRISON: And Howard, is it true that when you look across product lines, and the extent to which people retain older systems, or older products, that in the computer world there is a much higher retention rate among older systems?

MR. SCHMIDT: Well, I think it goes two ways. It depends on your penchant for technology. I'm the proverbial early adopter. I'm the one that will buy a $600 piece of equipment, knowing in six months it's going to sell for $49.95. And those of us that are of that ilk, we obviously will continuously upgrade.

You will have sort of the middle range, where people will have a family computer that, as the prices continue to go down, the experience becomes more rich, more robust. They will pass that on to the kids as their computer, as they buy themselves a new one.

So we will see some migration of some of the products, but often times we will see some people that

say, "Hey, it works. I like it. I don't want to change it, I'm afraid to do something different," so they will keep the hardware and software longer.

MS. GARRISON: And are there any special problems in terms of security of information with disposal of old computers?

MR. SCHMIDT: Well, now that you mention it, that's a concern especially in a consumer environment, but even more so in the corporate environment. Many times people will just turn their old computers in, recycle them, and personal data is sitting on the hard drives.

So, by developing a process before you turn it out -- it's almost like the analog, the paper world now. Shredders are selling at this unbelievable rate. There's a TV commercial saying, "Here, protect your information by buying a shredder." We see that now.

Same thing, electronically, we have to remember that much of that data on your computer is accessible, even if you reformat the hard drive. You have got to take some steps to wipe it out completely before you turn it in to a salvage operation.

MS. GARRISON: Thanks. Alan, do you have anything to add to that?

MR. PALLER: No, I think he did a great job.

MS. GARRISON: All right. Andrew, do you want to speak very briefly about password vulnerabilities? We heard an awful lot about it in the earlier panel.

MR. PATRICK: We heard a lot about passwords. I just wanted to add one other thing, which was we talked a lot about users and users' password behaviors -- writing them down, forgetting them, sharing them. We should also talk a little bit about what can be done from an operator's point of view, in terms of making password systems more usable and more secure.

For example, practices like forcing password changes immediately are very bad practices. People don't forget on demand, and so asking them to immediately choose a new password -- forget the old one and remember the new one -- is just a very bad practice. You get much better password choice and password remembering if you give people warning.

Obviously, asking for multiple passwords, especially when they're not absolutely necessary can be a concern. We have talked about having clear password rules, teaching people how to make good passwords. There is a lot of software around that will look at passwords as people choose them, and make recommendations on those, and that software is not used very much. So, if people enter weak passwords, they can get feedback from the

software immediately, before that password is accepted. Those kinds of practices can really help.

There is a reason why people share passwords. They write them down and they share them because, often, the work requires the sharing of information. If you're operating systems that don't support information sharing, such as sharing of documents across users, if you're operating a system that doesn't support people who may forget their passwords, if you don't plan for password forgetting, then it's no wonder that people start writing them down.

If there is at all a high cost, such as social or work or otherwise, for users forgetting a password, of course they're going to write it down. So if you don't have 24/7 password support, or an easy way for people to get their passwords reset, what are they going to do? Of course they're going to write it down.

Although passwords are weak, they are weak for a reason. Users' behavior with passwords has been well studied. There are lots of things that can be done here, and it really can be summarized in focusing on three questions.

You have to consider teaching the users why good passwords are important. Many people feel that they are a small cog in an organization, and so their

particular password may not mean very much. But we know that a small vulnerability can be a large vulnerability.

So, you have to answer the question why. Why do I need a good password? You have to answer the question how. How do I create a good password? You have to show examples, get feedback, and support passwords that allow people to get the job done, such as group passwords and work sharing.

And finally, you have to answer the question of how many, and we have talked about that. You really have to think about how many passwords, and what you're really asking people to remember, and realizing that they are not going to remember it, they're going to do something else. And until you have solutions like single sign-on, and whatever, realize that people are just being asked to do too many.

MS. GARRISON: Thank you. Alan, I would like to ask you what are the principal threats that weak security causes for home users? Is it primarily that hackers can steal personal information for identity theft? And what can consumers do, technologically or otherwise, to protect themselves?

MR. PALLER: I think what you described as the principal threat is the one that's most often called up when somebody is trying to sell people security, it's

almost never the real threat. There are three real threats.

But before I answer the question, today is actually a celebration day in the security field. Listening to Jim talking about ISPs in a sense competing for who has got the better security offerings -- not all of your ISPs have all of the services, and then Comcast says, "And we have these" -- that's a huge change.

And the man sitting over there, and the man sitting over there, and Dick Clark all get enormous credit for changing the marketplace to where the consumers expect it. It wasn't you saying it to the vendors that changed anything. It was you saying it to the consumers and the consumers saying it to the vendors and then the vendors said, "Oh, well, our customers want it."

And listening to Dell talking about what they're doing, it's a massive shift in everything, and I think there are some bows that you all should take.

Having said that, there are still some threats. Everything is getting better, much better, but there are still some problems. And the problems, actually, are not quite solved by what we have heard, so I want to talk about three threats to the home user.

The most common one is their machines are being

taken over, generally, by automated software, or by downloading something that they shouldn't have downloaded. Often, their kids do the downloading, and it's on the parents' computer. So it's not quite the user who could be educated, it's the kid you wouldn't want to give a driver's license to being out and doing things.

That's happening at the rate of what we believe is between 30,000 and 50,000 a week. And honestly, I couldn't care less. Meaning if 30,000 people get their computers taken over and they have all got trouble, it wouldn't matter, except we have got a different problem, and that problem is -- well, let me talk about when they learn about it.

The way they learn about it is either somebody puts pornography on that system they took over, or they put software on it, or they used that computer to attack the Defense Department. And the way they hear about it is when the FBI knocks on their door and says, "Why is your computer attacking DSA?"

And I asked the head of the FBI's cyber crime unit in Baltimore, "Does that happen very often?" And he said, "Alan, all the time." And then he paused, and he said, "All the time."

So, this is not uncommon, and that's a bad

thing, that's bad. But that's not what I'm worried about. I am worried about it because, as you will all learn later in the summer, somewhere between 500,000 and 1,000,000 machines taken over is sufficient to take the Internet down and keep it down. And 30,000 to 50,000 a week doesn't divide that badly into 1,000,000. And that's the reason we care.

And so, when I tell Phil that I worry about the older machines, and I don't just worry about the new machines that are coming out, you've got to do something for me about the older machines -- it isn't because I'm worried about somebody losing their personal data. It's that I don't want another 30,000 machines being taken over by somebody who can use them in a concerted fashion to attack what we think of as our e-commerce engine.

The other two threats, though, real quickly, are that the attacker can damage your computer. This happens a lot with Kazaa and other things, but that software can actually take you out, and you can't do anything. And your machine dies, and the idea of backups for most of us is a foreign term, it's not English, we don't know what it is.

So, cleaning the machine up and getting it back is really a very difficult thing. And just as an example, of the 150,000 machines that were taken over

with Code Red, we think about 30,000 are still just as infected as they were before, because it's so much trouble to clean up. And the reason we know that is there are about 30,000 machines out there trying to infect other people, so it's likely.

But the last one that I think is important as a real threat -- you all have heard of VPN, virtual private networks, and you think, wow, cool security system. I can use the Internet, I can sit at my home, go through the safe system, and get to my computer.

It turns out that's right, but there are lots of cases where the attackers know this. They infect your machine, and if you think you're smart enough to beat being infected, challenge me some time. They take over your machine because they know you're an employee of the Justice Department or employee of DEA, or an employee of something else, and then once they have your machine, they have a complete open pipe to the Justice Department's machine. It's not a secure pipe, where there is security, it's actually an open, fully open pipe. That's what a VPN is, it's an encrypted open pipe.

So, those are the three risks. Your machine gets taken over and the FBI comes knocking on your door. Your machine gets broken, and your machine gets taken over and they use that to get to your employer, your

employer finds out, he is a very unhappy person. Those are the three main reasons.

MS. GARRISON: Frank, I wondered if you could add to that, and answer the question what can consumers do, technologically, to protect themselves from these threats?

MR. REEDER: There is a risk of being on the last panel at the end of the day, and that is repeating everything you have heard before, but that's just about everything that has been said. So let me avoid saying that, by adding a "me, too," and hit a couple of points.

First -- and here, Andrew, you were very helpful in an earlier panel, in suggesting that we are using "transparency" in two very different ways -- and let me suggest, without going back to Descartes, that, in fact, when we use "transparency" in the sense of something happening without our having to intervene, let's think of that as being passive, as opposed to active security.

And I would argue in the consumer space, for all of the reasons that were discussed on the second panel this morning, the notion of expecting consumers actively to be chief information security officers of their own desk tops or of their home networks, I would argue, is hopelessly naive.

So when we talk about what the consumer can do, the short answer is buy safe products. The barriers to that are, I would argue, twofold.

One is -- and they have both been touched on -- the age of the installed base, the difficulty in doing that for old technology, and second, the complexity of what we're doing with the result that accountability is diffused.

Dean Mark Grady, at George Mason Law School, talks about why tort law won't have the same effect in cyberspace that it has had in other consumer areas, largely because the finger pointing looks like this.

Like Alan, I am delighted to see the ISPs stepping up. I am thrilled, not only because it's based on work that the Center for Internet Security has done, that we are starting to see ISPs, we're starting to see equipment manufacturers like Dell, we're starting to see software vendors make safety security a feature.

I think the simplest thing that we can do -- and I think here the Federal Trade Commission can be enormously helpful -- is begin to identify a set of things that represents safe products, and then validate claims that vendors make that their products are, indeed, safe -- essentially, a truth in advertising role, rather than a regulatory role.

This is not a polemic against teaching safe computing or strong passwords, but I would argue that the notion that such practices will become pervasive in the short run, I think, is -- let me be slightly provocative -- hopelessly naive, which is not to suggest that we shouldn't do it.

It's not obvious to me even that passwords represent a serious threat, because nobody has shown me any data that break-ins into home computers have resulted in any serious losses. The losses occur because of viruses which have nothing to do with secret passwords, or the difficulty of passwords.

So, that's where I think we can be of help to the consumers, by starting to produce, as we are hearing today both from the software vendors, from the hardware vendors, and from the ISPs, safer products and services that are clearly identified to the consumers, so that consumers, in the marketplace, can make those choices with reasonable assurance that the claims being made are as advertised.

MS. GARRISON: Well, your comment about benchmarks I think leads us into the big question for this panel, and Howard, I would like to ask you to initiate the broader discussion.

What mechanisms allow us to achieve the goal of

a culture of security, and specifically, how do the adoption of security benchmarks help in this regard? Or, are there additional incentives needed to encourage development of safer computing tools and practices?

MR. SCHMIDT: Well, I think first and foremost, there is a tremendous number of incentives out there. Just from the consumer perspective, we want to enjoy the experience. We want to be able to feel secure in our purchases, we want to be able to feel secure in our research that we're doing online. So there is an incentive for us to learn more.

Now, what are the mechanisms? First and foremost, I think the mechanisms that are in place have been described. The ISPs are not only looking to remove that burden from the consumer space, but they're looking to do it in a rather rapid fashion. So that helps move the culture of security to the backs of those that can better handle it.

The education, training, and awareness component, whether it's the FTC website with Dewey, or Stay Safe Online, or the individual vendors that have security and privacy sites out there. Those are some of the mechanisms that, once again, are just as routine as buckling your seat belt, or making sure you have an airbag in your car as you move forward.

The other thing is this automated process for updating of anti-virus software, personal firewall signatures, those sort of things.

And the last one is just learning about security and privacy, how things work. You know, it's interesting. As I learned how to drive, I learned that the big one was the one that made you go fast, and the short one next to it made you stop. We need to do that more in the online world, and make sure people understand. "Here are the things that will make you go good, and here are the things that will cause problems for you."

MS. GARRISON: Thank you very much. Any other comments from any panelist?

MR. PALLER: I think Rich Lloyd -- since some of you weren't here when the Dell representative was talking -- Rich Lloyd said this morning that they couldn't have done the new system, safer system, if he hadn't had independent benchmarks.

You can't ask every vendor to develop their own standards of what means safety. And so, I think it is the consensus, the government and industry consensus, on what a safe home system is, what a safe workstation is, what a safe web server is, that allows people to deliver them that way, and I think the same thing will happen

with ISPs. Determining what a safe ISP service is will allow the ISPs to all get to it really quickly.

MS. GARRISON: Jerry?

MR. LEWIS: Yes, just a quick follow-up on Alan's earlier point, which I agree with completely. Consumers have definitely told us and other ISPs, "We want security, we want privacy," and we have certainly responded.

And you know, the situation he posited about a zombie computer attacking the Defense Department, that's something that draws resources off the Secret Service, or the FBI, and it's certainly something that draws resources off the ISPs.

We have lots of those zombie computers that show up on the abuse team's radar screen, and it's often an old machine with Code Red trying to port scan somebody else, to infect them. It draws a tremendous amount of resources and dollars and time on our part, that we could be spending doing other things to help protect our customers.

And some of it is legacy systems, some of it is just bad consumer behavior, some of it is just completely unknowing consumer behavior -- the kid home from college downloads a lot of files, goes back to school, and the parents are left holding the computer.

So a tremendous amount of resources that goes into that. And part of why we think better security, both at our end and at the consumer end is a good thing, is that it helps us reduce our cost and our expense of dealing with these kinds of issues, and likewise, can help the consumers reduce their frustration.

MS. GARRISON: Jim, just very briefly -- we, unfortunately, are out of time.

MR. HALPERT: I would just add that there is a great diversity of different situations in which consumers and business users access the Internet. And talking about what a safe ISP experience is will vary greatly, depending on whether it's a broadband connection, a dial-up connection, a narrow band, or a proprietary online service, which often has a greater security environment, because all traffic has to go through one place in the network, typically.

And it's very important, as we think about these, that we understand what the security challenges are, and whether the standards are sufficient to meet those challenges.

Also, as we have heard repeatedly, security needs to evolve. And the notion that we can just establish a benchmark and sit on it may actually lead to less security, because security has to be dynamic.

And we need to have a sophisticated understanding when we talk about what these things mean -- and they really are a lot more complicated than just having one single stamp of approval. FTC deception authority, making sure that when vendors are selling products and saying that they are secure, they really are secure, is a very, very important role, and one that ISPs, as purchasers -- really, as middlemen, who simply purchase this technology and pass it along, as you heard from Jerry -- need to depend on, as well.

So, we applaud the FTC's role so far in its security work, and look forward to working with you in the future.

MS. GARRISON: On that note, I am afraid that we have run out of time. And I would like, at this point, to thank the panel very, very much for a fascinating and informative discussion. Obviously, we need to continue this another day.

I would like to introduce Howard Beales, the Director of the Bureau of Consumer Protection, who will make closing remarks.

CLOSING REMARKS

MR. BEALES: Thank you, Loretta, and thanks to all of you. This has been an extraordinary program. I want to thank the panelists, and I want to thank the FTC staff, who made it all possible. As the day concludes, I think that we're all walking away with a better sense of the role that technology is playing in this area, as well as how it can be made more effective as a consumer tool.

We began the day by reviewing the privacy-enhancing technologies that were available to consumers during the last decade, and examining what has succeeded and what has not, and why.

Many of the early technologies were difficult for consumers to use, because the process took too many steps, or it was hard to understand. And consumers did not want to pay separately for a fix that many assumed was already integrated into the computers and applications that they purchased.

Some anti-virus software, or firewalls, had the added burden of requiring active monitoring by consumers for updates and patches. Sometimes security software was also incompatible with consumers' existing applications or operating systems, especially if they have older computers.

All of this can be very frustrating and

overwhelming, especially to the number of consumers who are non-techies. The lessons from these experiences is that to be successful in the future, these technologies need to be easier for consumers to use, and built into their software and hardware. Otherwise, consumers won't use them, or if they do, they may not get the full benefit of the protections.

Academics who have studied consumer behavior in this area provided additional insight about how to increase the effectiveness of technology in protecting personal information.

For example, consumers may want to make different choices in different situations. It's difficult for them to focus on, and it's difficult for them to make global decisions about how information should be collected and used. Timing is everything.

The information that is given at the time of a specific transaction is likely to be much more effective in guiding decision-making than information that is presented in the abstract.

We also heard about factors that build trust online. These include ease of navigation, brand name, recommendations from others, the particular type of industry. Perhaps most important was the superficial look of a site. How the site looks, the colors, the

fonts, how professional it seems.

Now, that's at least a little disturbing, particularly in the context of our fraud cases. But unfortunately, it seems to be true. But it also creates an opportunity for manufacturers and vendors who are developing and marketing privacy technologies to do it in a way that appeals to consumers.

Technology is only part of the picture. Many of the strategies consumers should use to protect themselves don't involve the purchase of new or separate products, or services.

So, for example, consumers should know who they're dealing with before they give out personal information. They should not open e-mails -- and especially attachments -- from senders they don't recognize. They should use passwords effectively by combining letters with symbols, and keeping them in a safe place.

Clearly, however, the more things we ask consumers to do, the harder the task becomes. That's why technological solutions, where protections are built in and activation is simple, offer so much promise in helping consumers to protect themselves.

For managing digital identities, panelists examined various identity management systems, including

single sign-on, biometrics, and smart cards. We also examined recent work to develop principles in this area by the National Academy of Sciences, and by CDT.

We are clearly at a transition point, as we move to these more high-tech systems to identify us in so many of our daily activities. It's important to engage in a dialogue about how to build in protections at this early stage. It will only get harder if we wait.

Finally, we looked at safer computing, and what progress has been made in the last year in promoting a culture of security.

Some of us remember there was considerable discussion at last year's workshop, as at this one, about the needs for products and services that have built-in protections, which are automatic and easy to use.

Today, we learned that industry has begun to respond to this challenge, and that security technology is increasingly incorporated into the system by design, and not as an afterthought. For example, some ISPs have started to provide services with firewalls and virus protections included, as part of the package.

Panelists also discussed the importance of security benchmarks, such as those developed by the Center for Internet Security, which are already being implemented by at least one company.

So, thanks for coming. We hope to see you back on June 4th, when we will continue our discussion by focusing on the challenges that businesses face in protecting the information that they collect and maintain about consumers. I thank you all, and we will see you on June 4th.

(Applause.)

MS. GARRISON: Before we conclude, Commissioner Swindle has some remarks.

COMMISSIONER SWINDLE: I figure those of you who are still here are so damn tired you can't get out, and I might as well talk to you while you are here, a captive audience -- I am convinced we do have Baptists in the audience. You are so spread out from the main pulpit here, that you know, the preacher always reaches out to grab you.

I just want to make a few remarks of appreciation. First, Loretta, Toby, and James and the staff that worked on this, we had a great successful workshop here a week ago, I guess it was, and we've got another one, a smaller audience, but a different kind of an audience. I know I can speak for Tim and Howard, who has already said it, thank you so much for coming and hanging around and being a part, but more importantly, really contributing to this overall effort.

As I said, and was paraphrased here, this effort is not a destination. It's a journey, and we have all got to walk along that path, and we have got a lot of stuff to do.

I am really impressed with some of the accomplishments that have been discussed here. You know, we have had some great companies in here talking today. We have had Microsoft and Dell and others, and I, unfortunately, had to miss portions of it. But the things that are being done by great companies in a great country are getting it done.

And as Andrew says, we ain't there yet, and we're not going to get there. If you're thinking we're going to find that we wind up somewhere and take our pack off and say, "Hey, guys, we did it," forget it. It's not going to happen.

And the way we're going to accelerate the journey and accomplish more during the journey is for Alan Paller and Andrew and all the non-government organizations to just keep the pressure up. As Alan said, we've got consumers now paying attention to this, and guess what? When consumers pay attention to it, big companies, big great companies, they pay attention, too.

And Jerry, I thank you so much. I am very familiar with Comcast. I was on Excite@home, and we all

went through that disaster. And they have come so far.

And things are different today, as several have pointed out, we are making progress. And you know, Howard Schmidt here, a dear friend of mine, and what a hell of a loss to the U.S. government for him to depart the scene -- but I know he's not very far away, and when we get in trouble, we will call him and he will come back -- but it's great to have him here.

Philip, Microsoft, great company. Would you please spend some time with me and tell me how I can stop these incessant messenger pop-up ads that I'm getting here in the past two weeks? I want a solution to that, or you can't leave the room. So that is high priority for a great company. You don't want an unhappy me.

(Laughter.)

COMMISSIONER SWINDLE: But seriously, Frank, I've got to comment on your saying that maybe consumers can't handle all this stuff. And I agree. This is all complicated stuff. Hell, I can't even get home usually by myself. It is a problem.

But I remember back when Henry Ford rolled out his first car. I'm the only one here old enough to say that. And there were people saying, "Oh, my God, you can't turn these dangerous vehicles -- they are very complicated, you can't turn them loose with the

consumers."

And then, when I was a young aviator -- before I was an aviator, they came up with the airplane, and we rolled those suckers out, and they said, "Good Lord, you know, you can't do that. You can't turn those over to normal human beings, you have to be elite to do this." And you know, I remember one of the first rules they gave us when we started flying, they said, "Never depart the boundaries of the air."

(Laughter.)

COMMISSIONER SWINDLE: It's really bad when you do that, you know? But guess what? We did it. You know, we have got millions of cars flying around here, and yes, we crash a few every year, but isn't it amazing? It's like a beehive. It works.

I contend consumers can handle some of this stuff, and it won't be at the sophisticated level of a Microsoft, or a Sun, or whoever else, or IT center here at the Federal Trade Commission. But we can handle this, as consumers, we can do certain basic things that will take 80 percent of the risk out of it -- the vulnerability out of it.

I remember my early days in the Marine Corps, when I really can remember -- I couldn't remember those first two things; I lied there, but back to the

confidence thing -- but in the Marine Corps, as a lieutenant colonel, just before retiring, I saw a personal computer. I actually saw one of these things. I had never seen one.

We had a computer center, it had these big machines, and they whirred, and they had air conditioning, and those floors, that you lift up the panels, and all this stuff, and we were not -- us common folks were not even allowed to come in that room. And it was about 60 degrees in that room. I remember I did sneak in once. They ran me out, because I wasn't cleared for that.

We had a policy that there would be no proliferation of computers beyond the computer people, because guess what? The common people couldn't be trusted with them. Now, virtually every household in America has a small computer, and it's a hell of a lot more powerful than those big roomfuls than we had back there.

We can do this. We are going to do it because great companies and great non-government organizations are going to lead the way. The government is going to be here to hold workshops and facilitate things, and start fights, and things like that.

But you're going to lead the way. That's the

only way. That's the American way. And thank you very much for being here with us.

MS. GARRISON: Thank you.

(Applause.)

MS. GARRISON: Thank you very much, and a special thanks to this panel, again, for their being here, and for such a provocative discussion.

We look forward to seeing all of you on June 4, for a continuation of this discussion.

(Whereupon, at 5:46 p.m., the meeting was concluded.)

* * * * *

C E R T I F I C A T I O N O F R E P O R T E R

DOCKET/FILE NUMBER: P034808

CASE TITLE: TECHNOLOGY WORKSHOP

HEARING DATE: May 14, 2003

I HEREBY CERTIFY that the transcript contained herein is a full and accurate transcript of the notes taken by me at the hearing on the above cause before the FEDERAL TRADE COMMISSION to the best of my knowledge and belief.

DATED: MAY 20, 2003

PETER K. SHONERD

C E R T I F I C A T I O N O F P R O O F R E A D E R

I HEREBY CERTIFY that I proofread the transcript for accuracy in spelling, hyphenation, punctuation and format.

SARA J. VANCE