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.)