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

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

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

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

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

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

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

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

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

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

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

MS. PERRIN: It will go on the record.

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

MS. PERRIN: Thanks very much, Toby.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

database of people's biometric identification.

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

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

MS. LEVIN: We will give you two.

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

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

I mean, you still have to train your kids not

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

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

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

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

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

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

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

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

MS. LEVIN: Thanks, Stephanie. Excellent.

(Applause.)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Act.

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

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

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

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

colleagues.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

the individuals to be aware of the cost.

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

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

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

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

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

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

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

So, it's not just about money --

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

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

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

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

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

MS. LEVIN: Alan --

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

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

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

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

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

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

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

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

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

MS. LEVIN: Good additions. Alan?

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

And maybe that tells us something, which is

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

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

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

MS. LEVIN: Lorrie?

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

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

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

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

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

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

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

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

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

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

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

MS. LEVIN: Okay.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

to go and look up the complete studies.

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

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

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

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

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

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

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

could easily be fixed in a future version.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

lot more detail in the report.

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

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

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

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

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

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

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

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

MS. LEVIN: Thanks, Lorrie.

(Applause.)

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

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

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

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

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

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

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

actually surpassing them.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

MR. WEITZNER: All that?

MS. LEVIN: From your perspective?

(Laughter.)

MS. LEVIN: All that, and more.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(Laughter.)

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

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

MS. LEVIN: Marty?

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

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

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

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

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

(No response.)

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

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

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

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

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

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

PARTICIPANT: There you are.

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

MS. LEVIN: Okay, very good.

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

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

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

I arrived home about a month ago to find my

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

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

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

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

looking more and more at that issue throughout the day.

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

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

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

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

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

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

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

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

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

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

that, I think, are major benefits.

MS. LEVIN: Okay. Next question?

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

MS. LEVIN: Okay, thank you. Joe?

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

and expense.

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

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

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

(Applause.)

(A brief recess was taken.)