still some food out there, a bathroom break, and then rush on back. Thanks.

(A brief recess was taken.)

PANEL 2: Business Tools for Protecting Consumer Information

MR. SILVER: This is the second panel. We're going to learn about some technologies currently available to businesses to help them protect their systems and information.

Where appropriate, if the panelists feel like it, I'd ask them to perhaps reference the previous hypothetical, if it's natural. References to Larry's mom or Gary's dad will earn extra credit, as well.

The biographies of the panelists are in your folders, but I will give brief introductions.

Joseph Alhadeff returns from his acting debut in the previous panel. He's with Oracle.

Christopher Klaus is from Internet Security Systems.

Gary Clayton is not here yet, but he's from Privacy Council.

Christine Varney is counsel to Liberty Alliance.

Toby Levin will be assisting me in this panel. She's at the FTC.

Ari Schwartz is with the Center for Democracy and Technology.

Michael Weider is from Watchfire.

Craig Lowery is with Dell.

Steven Adler is from IBM Tivoli Security & Privacy Software.

And Robert Gratchner is with Intel.

You may think first of software when considering privacy and security tools, but Robert will lead us off with some remarks on a tool that consists not only of software but actually hardware, as well.

MR. GRATCHNER: Can everyone hear me okay? I'll try to keep my comments on Larry's mom at a minimum and see if she can understand this technology by the end of my discussion today.

I first want to thank the FTC for putting this workshop together and allowing all of us today to come together and discuss technology and how it affects business. It's a great opportunity to be here today and to talk to you all.

So, my first few slides today are basically talking about the environment and situations that businesses face.

I also want to let the panel, if they have any additional comments on this, to feel free to chime in on this during my presentation or afterwards. Comments or help to clarify points are always appreciated.

So, this first slide I want to discuss is actually what are we trying to protect and what are the layers of protection?

Obviously, the core of what we're trying to do and identify is the data, the personal identifiable information, and surrounding that data is applications, the operating software, the actual applications using and manipulating that data.

Surrounding that is the infrastructure, the actual hardware, the PC or the hardware incorporating that, and surrounding that is the network, the final layer of protection.

And the point I want to get across here is any weakness to a layer of protection can expose that information.

So, a weakness in the infrastructure could lead to exposure of that data.

We need to make sure that the fence around that data and around those layers of protection is strong and it encompasses all.

Talking about the environment that we're facing today as corporations, we talk about individuals, devices, a firewall, and a network, individuals being employees, customers, vendors, suppliers, who have access into data.

They're using devices like PDA's, PC's, cell phones.

So, all of these types of devices have to be considered and understood within the environment.

With regard to software, we’re it's talking about the operating system. We’re talking about anti-virus software.

Most businesses use a type of firewall before anyone can get into their network.

Then once you get in the network, we're talking about servers, routers, switches, and all that.

But the most important piece -- and they alluded to it a little bit in the earlier panel this morning as the business processes, is talking about policies, ensuring employees are trained, ensuring that there is enforcement, that there are guidelines out there, and that these guidelines then are followed through and the companies are following those, that there is the actual penetration testing that we're seeing and emulating what hackers may do. Then obviously the most important, for me as an ex-auditor, is the risk assessment. What are the risks that business are facing?

And a breakdown in the business processes, to me, can lead to a breakdown in any of those individual environments, whether it be devices, firewalls, or network, because they're all interlaid and intertwined by this business process.

And finally, the last slide on the kind of the environment is what is the safer computing initiative going on today and in the future?

In the past, it has been software only. It has been anti-viruses, the use of passwords, VPN firewalls.

There has been the emergence of the technology of smart cards. At the May panel discussion, there was a pretty good overview of smart cards and their technology and the use of smart cards. That just adds another layer of protection.

Currently there's another technology, which I'll talk about a little later, called TPM, trusted platform module, which performs platform authentication in fixed hardware. This is a technology that's starting to emerge.

There's current platforms right now which incorporate this technology.

And for the future, one of the things that we're working on at Intel is LeGrande technology, which I'll talk about more, is a hardware solution.

Who knows what’s in store for the future, but obviously, we're seeing a need to better secure data. By adding all these technologies together, we're eventually, hopefully, going to get there.

So, the TPM solution is, at the most basic level, a smart card on your platform or on your mother board.

It acts with the ability to do cryptographic key encryption, and it also performs platform integrity testing.

The TPM is done by a group called Trusted Computer Group, an open forum group to anyone who wants to participate, which is putting together specifications to allow these two types of capabilities.

It's intertwined with the IO controller hub, which goes within the chip set, which then works with the processor.

It can work with a portable token or a smart card, and the important part with regard to privacy in the TPM is, from the onset, this organization has considered privacy. Privacy was very important in the processes and in the consideration of developing this technology.

The Trusted Computer Group has a website. You can go to that website, see data, see the white papers, and all of that is open to the public at large.

So, with regard to LeGrande technology and what Intel has been working on, LeGrande basically is a hardware-based solution for security technology.

It's operating system-independent. The goal is to work with any type of operating system.

Basically, it's going to create protected data paths.

It's going to protect execution environments within the processor and protect key operations and storage to basically help strengthen the encryption capabilities within the processor.

Now, once again, within LeGrande technology, privacy has also been considered in the development. The privacy team has been working with the product development team to ensure that privacy is considered at the onset and integrated into their processes.

We shipped this out to our manufacturers with these capabilities.

So there are two types of users with LeGrande technology.

There's the owners, the people who actually will buy the technology, and these can be your IT shops or this could be your PC person at home who actually bought and owned the technology.

Two is the user, and the user is the person who's actually using the machine. So, this could be an employee of the company or it could be another family member who is using this technology.

But basically, the owner has the ability to opt in to this technology when they're using it. The user also has the choice to use this technology or not to use it. Users also know when they're in a protected state and when this technology is being utilized at all times.

The bottom line when we were working with the team, is that we want to make sure that we strengthen the security of the users without compromising their privacy.

To sum this all up, in talking about the LeGrande technology, we want to improve security without compromising privacy. There is a uniqueness within the TPM, which is not manufactured by Intel but was defined by these specs, by this organization, but then developed by other companies. There is this privacy model, an in-depth privacy model that they are using and working with, that has been reviewed and can be reviewed by people outside.

It operates on private information data out of the view of other software, so that this is totally protected and cannot be witnessed by malicious users or malicious outside sources.

It empowers the choice of the user, and it's independent of any type of operating system or application. The bottom line is that it is designed to enhance computer experience by increasing security.

Thank you.

MR. SILVER: Thanks, Robert.

Let's talk about another new system now. The Liberty Alliance Project is developing a specification that could change how information is shared within companies and also between companies and consumers online.

Christine Varney will explain how deployment of this specification could provide a way to protection in consumer information.

MS. VARNEY: I was going to ask Robert to put his first slide back up and then show you where Liberty can sit.

Thank you so much, and thanks for inviting me. I was commenting to Toby, we've come a long way from the days when some people thought that privacy was not a issue for consumer protection.

What was that, Toby, in '94 and '95?

And now they even have this wonderful coffee and food outside.

Thank you. I know some of the business people here provided it.

The evolution of privacy has led to some really interesting technological evolutions, as well. What Liberty is doing is playing in the space that Robert has in the blue and in the brown, between the two, and let me explain that to you.

Liberty Alliance is a specification body. As consumers, you will never hear about Liberty. You shouldn't. It is a back-end specification body like HTTP and HTML, SOAP, SAML.

Liberty is like Oasis or like the Internet Engineering Task Force or any of the other 200 bodies that create specifications upon which applications can be developed.

Liberty came into being with a vision of creating an open, inter-operable, decentralized system for federated identity and authentication.

Now, the reason that's important is, if you think of a best case scenario for consumers who choose it, for people like me who travel a lot. The reason that planes are always full nowadays is because they're canceling flights left and right.

So, imagine a scenario where you're extremely busy and you've got flights, you've got a car picking you up, you've got a meeting at the other end, you've got a hotel reservation.

Imagine a system that you have chosen to participate in, affirmatively, that allows all of the enterprises that you're engaged with to talk to each other.

So, United sends the message out through my calendaring and messaging system, that my plane has been delayed.

It contacts the car service I use and says pick her up later, her plane has been delayed; it contacts the car service on the other end to pick her up later, her car has been delayed; it contacts the hotel, if it's a guaranteed time reservation, and says hold the reservation, she is going to be late; and contacts the people I'm meeting with. It does the whole thing. Down the road, my identity manager can look around for a different flight and see if there's another flight that's going to be more convenient for me and notify me.

There are all kinds of convergence in a loose sense that a lot of technologists -- and I don't know who in the room is a hard-core technologist; Richard is not here at the moment -- that technologists can envision down the road -- these seamless conveniences both for consumers and for enterprises.

Right now, suppose you wanted to go through the example that I just did. Hypothetically speaking, say I had a United Airlines flight and a Hertz rental car and I was staying at a Holiday Inn chain. If those companies wanted to offer me that kind of convenience, what they would actually have to do is go write software that would allow their systems to talk to each other. Nothing like that exists today, nor could it exist because everybody's systems are proprietary.

So, the idea behind Liberty -- and it's very critical for e-wallets -- is that there are products out there that are very nascent, that are beginning to offer these kinds of services. For the most part, they are proprietary and they are centralized, so that if anyone wants to get access to your data, all of the data is kept in one database or in databases that talk to each other.

The idea behind Liberty is why don't we create a specification that companies who want to can build applications upon. The premise of the specification is that it's open, it's published, it's at www.projectliberty.org. We're on version 2 of the specification now. And it's royalty-free. Anybody can write applications on top of it. And it's decentralized, which means that your data -- and I'm going to keep using consumer examples -- your data doesn't have to be centrally stored anywhere for this system to work.

I‘m going to make a very rough analogy, so if there's a technologist in the room, stand up and tell me how to give it a better translation. The rough analogy is think of it as peer to peer for your data, where you may choose to keep highly confidential trust information at one source, whether that is an American Express or a Morgan Stanley or a Bank of America.

You may choose to keep less confidential data maybe at Yahoo. The data that you would need for a variety of systems and services to work would be kept separately at various points in what Liberty calls a circle of trust. So when you want to make a call on the data, in our Liberty world, the identity provider goes out and makes a call across all of the members of the circle of trust to find the data that's needed and relevant for the transaction and brings the data back to complete whatever the transaction is.

The idea is very simple. In a single web session, a consumer would be able to move around without re-authenticating, without using additional passwords or sign-on's or anything else, in an individual circle of trust or across circles of trust that have contracts with each other.

The way a circle of trust works is that a group of companies would get together and, by contract, agree that they were going to offer the consumer this service.

Hypothetically, say it's AOL, it's United, it's Hertz, it's Holiday Inn, and it's AmEx and Mastercard and Visa.

All of those companies would affiliate. They would sign contracts. They would create their circle of trust.

Now, you, the consumer, don't ever see any of this. Suppose you go onto AOL, and AOL says, hey, consumer, we have the ability to link your accounts between these companies.

Please let us know if you would like to link these accounts and if you would like the information to be shared between us and click here to see exactly what information gets shared, by who, for what purposes, under what circumstances -- the whole nine yards description.

Then if the consumer says yes, I want to do this, when you're in a web session, you can move around between anybody who's in the circle of trust. This is very convenient, again, in the travel industry, when you're trying to make travel reservations, you're trying to make hotel reservations, you're trying to make airplane reservations, you're trying to make car reservations, you're trying to get them all charged. It offers a lot of convenience.

So, what Liberty sees as probably the first commercial, consumer application that will probably evolve is likely to be the travel space.

As the e-wallet space matures, we're likely to begin to see some applications there.

Before you see that, what's happening right now, as we speak, is that Liberty is being deployed in a couple of companies -- and I can't say who, but if you look at our members list, you could probably pretty easily guess. What happens with very large enterprises that have been around for a while -- and everybody in the room is going to be familiar with this -- is they have a legacy system.

So, you work at a company and -- you in the government will appreciate this -- you're trying to figure out, what's in your TSP account, you're trying to figure out how many hours you have accrued for vacation, you're trying to figure out what your salary is likely to be next year, just all kinds of data that you might want to have access to as an employee. In most corporations, if that information is available electronically to you, it's usually only partially available, it's usually hard to get at. Often you e-mail the right person and they e-mail you back.

There are probably half-a-dozen companies right now that are deploying applications in data based on the Liberty specifications because it's cross-platform, it works across multiple systems, and it works across legacy systems. So, it allows large corporations to be able to provide data to their employees from multiple sources.

Now, that's where the authentication comes in. This is very important if you're an individual, whether you're operating in the business world or in your employment world or in a consumer space, that you be able to ensure your data is kept safely and securely and that only the individuals or enterprises that you want to have access to it get access to it. The way that happens is through authentication protocols.

If you're moving about the web, you might have a very high level of authentication expectation for anybody who can get access to your bank account. You probably don't want to have a lot of people have access to that, and you probably don't want your bank to give it to a lot of people.

So, the bank will require a very high level of authentication.

You may want to check the local weather and sports on Yahoo, on My Yahoo, right? But you probably don't need a high level of authentication for that.

So, Liberty provides for any authentication level or technology that a deployer offers.

It's technology-neutral. You can put in any kind of authentication that you want, which goes back to some of the points Robert was making.

Liberty is a specification. It is only as secure as the Internet is right now, and there are a lot of vulnerabilities in the Internet.

It is also only as secure as the business deployment of the application is secure. Because Liberty writes specs only, they don't write business rules, and because they are working on the existing architecture of the Internet, they can't cure the security risks that exist in the Internet today.

You can go to the Liberty website and see version 1's release and version 1.1 and now we're on phase 2 which has just been released in draft. Liberty has put out probably half-a-dozen technical papers. They're mostly extremely technical, and they talk about how to build a Liberty deployment that's secure and safe and privacy-enhancing. But those are directed at technologists, and I, frankly, have a very difficult time reading them.

There is one document, though, that I would commend to you, and it's called the Privacy and Security Best Practices. That document is written for business people who are making the decisions around what kinds of services they want to offer. The hope is that the business people will talk to the technologists and that they will get the right kind of guidance around the levels of security and the levels of privacy that should be adopted in any business implementation.

Liberty is also based on an opt-in. You, as a deployer of Liberty, can't enable the service unless the box in the spec that says "consent obtained" is checked.

Now, obviously, there's nothing that can prevent a fraudulent enterprise from checking that box. But as we all know, that's something the FTC would frown on and would, hopefully, vigorously pursue.

So, it is based on opt-in, and it does allow for whatever level of authentication a deployer chooses to provide. I think, James and Toby, that's probably enough of the overview and we can get into more specific questions.

MR. SILVER: Thanks very much.

We're running a bit behind schedule, so I'd ask any panelist, if they want to just speak from their seat, that might save us a bit of time.

We can move now to enterprise technologies, and I know that Joseph Alhadeff has some remarks about roles and rules-based solutions, as well as out-sourcing possibilities for smaller businesses and how to get some privacy features out of existing technologies.

MR. ALHADEFF: Right. Thank you.

One of the things that we looked at in the hypothetical and one of the concepts that hopefully came through was a concept that privacy, security, confidentiality are not necessarily differentiated within business, are not necessarily differentiated by consumers, but are clearly differentiated in IT departments, usually, and sometimes in legal departments, as well. When you look at solutions, though, you need to look at all the factors.

If you're looking at any one factor, you're missing a large piece of the pie.

One of the things that we've tried to stress is that the solution, while technology plays a great facilitating role, is not just a technology solution. There are policies and there's some hard work that has to be done in it.

And part of the hard work is that it used to be a lot easier to look at technology solutions, because it was the M&M concept before. That kind of shell was the dividing line where you have to do protection. What was outside was bad, what was inside was good, and that was the definition. Well, these days, you have to also look at what's inside the technology shell. The shell doesn't work quite so well.

We have to go perhaps from the chocolate M&M with the soft inside that was a little too squishy to more of the peanut M&M, where the inside remains hard, as well. An example of what I mean by that is you can deploy different types of technology. Our technology goes across the stack. It could be CRM systems. It could be enterprise applications. It could be a database, what have you.

But if you deploy enterprise applications and you optimize them only for one thing -- let's say security -- you may actually be missing part of the boat. Security may have meant to you I want to make sure that no one who is not one of my employees can get access to this information, but that might not be appropriate from a privacy perspective. You may have to also ask the question, do these people need access to the information for their job function?

Do I have a set of concepts, business rules, and processes by which I understand who needs access to information and why? Do I have that map of data flows, which was used in the example early on as one of the consulting priorities. Have I figured out the data flows?

No matter how good your technology is, if you haven't done some thinking to learn what your data flows are, what your business needs are, then you can't deploy a technology solution, because you don't even understand your own business.

So part of the question is having the technology work in support of the business once the business has identified its needs, as well as the concerns and needs of its employees and its users.

When you look at the way things are going out, you can look at it at different parts of the exercise. If you go back to the other bullet slide -- Robert, there's a little bit of familiarity in the structure of your slide and this slide, and I apologize deeply for that level of familiarity without your advice. You have the concept of the customer facing and the enterprise facing. We’re going to be looking, from my point of view, a little more at the enterprise side, but it still has some of the customer facing aspects.

If you look at a company that has customer relationship management systems, the question is, are you thinking about preference management? Are you capturing that information from your customers and your users and your employees?

What are their preferences? How do they want you to interact with them? Because that's how you prove the value proposition. You make sure that that's beneficial.

Now, they're going to have some controls on their side that are beneficial, whether it's P3P, whether it's spam tools, whether it's cookie managers, whatever. But there's still something you can do on the enterprise side to make sure that you're capturing that information appropriately.

Once you've captured that information, the question is does the back end honor those preferences? One of the things that you have to do when you honor those preferences is to think, okay, how do I then make sure that things don't get sent out that this person doesn't want to get sent out? How does the sharing not occur that hasn't been appropriately mapped?

Do I have business rules that reflect this? Do I have policies that reflect this? Have I done training that reflects this?

Is my approach to this integrated? Have I then set my security parameters according to a number of those preferences?

In our case, this would be across both the application server technology and across the database technology.

You can set the role. You can define exactly what the role of the person who is accessing the information. What are their rights and privileges related to accessing? You can map that to the business rules related to that information.

You can also then look at an IE management and a privilege management situation, which is I've identified the person, I have authenticating mechanisms, I have a system of making sure that privilege management occurs, because it's great to say you've got strong authentication. All my employees, for instance, may have to use a digital signature.

Well, that's wonderful, but if I forgot to have an HR system that updates their privileges, then I've authenticated the person to be able to access the wrong information.

The fact that I can tell that Joe Alhadeff is Joe Alhadeff is nice, but if I don't have privilege management in place, then the fact that I'm me is meaningless, because I'm getting to see all the wrong data again.

Make sure that the access controls are granular. What is it that you can see? How deep can you make that division between what you can see and what you can't see? Are you mapping it across both function and geography?

What controls do you have? In the case of our database application, you can also have a function called label security, which can actually get some of those controls down to almost the data element level.

After that, then you have to figure out, well, I do want to have a little bit of confidence that my people are doing the right thing.

I've had the training, I have a compliance program, I have methodologies, but it's also nice to have some control.

So, your audit functions have to be turned on in such a way that you can capture some of this information.

You also have to have it done in such a way that you can set some controls on these policies. One of the things which they've just been launching is a concept called an internal controls manager. That's really been done in response to a lot of the requirements that have come out of Sarbanes-Oxley. It can also be used, to some extent, to address some of the requirements that 1386 may be coming up with, because it's, in some ways, a testing of your controls and an audit against them.

A lot of this is technology that exists in the database applications stack, and it's technology that we'd like to think we do it best, but it's common to a lot of platforms. A lot of people aren't thinking widely enough when they deploy their platforms.

It's great to say you want to buy some new technology and you want to try to get new technology out there. There's a lot of new technology that's very valuable, but there's a lot of existing technology that can be configured to be much more effective than it has been. Often the configuration, even if you buy new technology, is an important thing to think about, because everything has to work together. You don't just take paper out of the system and you're there.

That's not e-business in a responsible or an intelligent manner.

You haven't done process optimization. You're not really gaining the concepts of a total cost of ownership. You're not really moving the ball forward as much as you can.

It would be lovely to say that looking forward to the time of the Jetsons that you're going to just have the fatigue of pushing the button, which is always the solution, and the button can help. That technology is going to be very beneficial. But it has to work within the framework of the business, the imperatives of the business, and the needs of the people the business serves, whether they're employees or users.

Once you have it working in that context, then you have technology maximized, because the drivers are all of the correct drivers, not just a slice of those drivers. At that point, I'll leave it there.

MR. ADLER: About two years ago, we started out to do something different, to build some enterprise privacy technology that wouldn't be based on anything else that we had built before. We did that because privacy is about purpose.

Now, I come from IBM Tivoli Security Software, part of the IBM Software Group. We traditionally made security software -- identity management software, data synchronization, access control. We have a rich heritage in building security software.

But when we came to thinking about helping our customers figure out how to build privacy into IT systems, we had to take a departure from where we had come from from a security perspective.

Security is about operational control of data. I heard someone say “legacy systems.” I built the systems that collect the data, so I am going to determine how to protect the data. That's an organizational view.

I've got people who have job functions, who sit in roles, who belong to groups, and I'm going to allocate access control lists to the types of applications and resources they can touch.

Privacy is a little bit more democratic. It's about consent and purpose. How are we going to use the data? What are we going to do with the data? It requires a purpose-based authorization decision.

So, while we at Tivoli build security systems to identify or authenticate the individual, as Christine said, and, as Joe talked about, provide access control for authenticated people to resources, we put one more layer inside there. If you looked at the chart that Joe put up before, it said authentication, access control, authorization.

Tivoli Privacy Manager is a purpose-based data authorization system. That means we're evaluating requests for data based on context -- not content of the individual, but context of the decision.

Why do you want to use the data, and has the company agreed to that purpose? Have data subjects agreed to that purpose? Have they consented?

To do that, again, we had to think a little bit differently about data authorization. We worked with 28 companies in what's called the IBM Privacy Council, which I'll talk about a little bit later. We worked with these companies because we realized at the outset that we were building something, again, that was very new, and we didn't know enough about it. We wanted to make sure that as we built something as important as a privacy management technology, that we would work in collaboration with organizations that had enterprise privacy challenges, that would have the kinds of complex problems that we would want to solve.

And one of the biggest things that we heard from our customers at the outset was to make sure that whatever solution we brought to market would be open standards-based.

So, IBM Tivoli Privacy Manager is a kind of privacy middle-ware. Do you know what middle-ware is? It sits in the middle of other software, it connects things. Because it's a privacy middle-ware, because we're sitting in the midst of customers that have large diverse enterprises with lots of different systems that need to be connected from a data management perspective, we chose to base our policy language on P3P as an open standards-based application.

Now, I'm going to go through a little bit about what Privacy Manager is and how it works from a really high-level perspective.

So, fundamentally, we take a privacy policy or a data authorization policy the company has, and we convert it to P3P.

P3P is a rules language.

Ari can talk about it or Lorrie can talk about it in greater detail.

As a rules language, we're identifying three key components: groups of users who can use types of data for valid purposes.

We post that policy, to groups who can use data types for purposes, to a server that sits at the hub of the enterprise. It publishes this policy to transaction monitors that sit -- here's a techy word -- like a proxy in front of a database.

The proxy watches applications requesting data from the database.

Now, the database could be an Oracle database. It could be a Sequel database. It could be a DB2 database. It could be anything. For every request that comes in to the database, we evaluate is this person, data user, who belongs to this group, allowed to ask for this data type -- a field, a record, or a classification type -- for this purpose?

We do a single check. We scan the record, the request. We take a look at it. We let the request go to the database, and while the request is going to the database and being filled, we send the request down to the policy server and ask is this purpose allowed?

The policy server may come back and say, yes, that purpose is allowed, for example, direct marketing is allowed, that data user can request 5,000 records for the purpose of direct marketing.

We then do a second check, because that policy server is keeping a consent repository for the entire enterprise.

We're centralizing user preference and consent.

It's going to do a check against those 5,000 people. Did they consent to that purpose?

And if they did, when the data stream comes back, we let it go through. But if any of those people said no, I don't want you to use my name for direct marketing, we block it, and we return a null value, and we keep an audit log of all of this.

I'll show you how this works.

Let's say, fictionally, you make widgets and you have a really simplistic privacy policy like this. I apologize for the small type, but they're all like this.

(Laughter.)

MR. ADLER: And your privacy policy basically says we're going to collect some data from you and we're going to use it to take your order and invoice you and process your order and ship your order simple stuff, and oh, yeah, we're going to share it with third parties.

That's the small type at the bottom.

So this policy is a legal policy, but it already has some rules in it. I mean a policy is a set of obligations and rules.

So, from an IT perspective, in order for us to take that policy and embed it or to make IT systems understand it, we have to start parsing those sentences, reducing them to a dialect, a rules language.

This is a little bit of pseudo-code here. We're doing some sentence parsing. And I apologize for the bad colors on this lap-top, but you can see the widgets billing department is a group, address information is a data type, and charging your credit card for the purchases you made -- that's a purpose, and you can see further down, shipping, marketing. These are all groups, organizational groups within an organization, and then their data types and their purposes.

Well, in Privacy Manager, we have an editor, which is published online -- it's a free download, you can check it out -- which is designed to take those groups, data types, and purposes, and transform them into P3P that is a machine-readable XNL-based policy, and it's very simple. All you do is you go in, you identify the group, purpose, and data types, along with some other conditions like dispute resolution, et cetera, and those get aggregated or stuck together into rules statements:

billing credit card for purchases.

You can see the relationship back to the privacy policy.

Information to ship orders. These are just the statement names -- that is, the groups and the types and the purposes strung together. You might have 50, 150, 500 conditional statements that form an IT privacy or data authorization policy. This is what your IT systems are now going to read when they make authorization decisions with Privacy Manager.

All those different statements get put into a policy.

We though a lot about what it means to have a policy, because a lot of our customers told us that, well, they've bought lots of companies in the last few years and those companies had policy and they published them onto the web and nobody kept track of what they were and nobody remembers what their obligations were.

But the reality about privacy policies is that they're like an insurance policy -- privacy policies are very similar to insurance. Incidents always happen in the past, but they're not reported until the future.

If you had a policy three years ago and you've got somebody reporting a violation today, you need some institutional record about what did I say I was going to do three years ago and what did I do and what did they consent to?

In Privacy Manager, all of the policies have inception dates and expiration dates, and we track all the occurrences, to use an insurance term, all the events, all the incidents, all the data access requests for any individual from the moment they deposit data. If it's just a monitored system with the preexisting data for that policy period, when you make a new policy, the system treats it as a new policy that requires new consent and a new data log.

So, that's the policy side. That's that server that sits at the hub.

Now, we go out to the IT systems that are actually using data.

We've got to monitor them. We've got to figure out, okay, somebody is using an application, they're requesting data from a database, what's happening there?

So, what Privacy Manager does is it goes out to the database. This is a screen that shows what our transaction monitors look like.

It goes out to the database and it grabs all the field names from that database, the table definition, what all the field names are called.

This is an enterprise. This looks like an LDAP database here. There are some enterprise JAVA names. There's an address, EJB, address, city, country, et cetera.

We then go out to that policy server and we collect all the data classification types. In this case, it's very simple. It's PII or non-PII.

And what you can see on the screen is we're doing something that Joe was alluding to earlier. That's data classification.

We're classifying individual field names in one database with classification values.

Let's say you're a small company like Golden Oldies and you've only got five major databases.

One's an Oracle database, one's a DB2 database, one could be Oracle financial, and one could be a web-sphere portal.

You've got totally different field names in each one of those databases.

So, Privacy Manager, by mapping those different field names to a set of common classification values, allows you to manage different systems the same way.

MR. SILVER: Steven, two more minutes.

MR. ADLER: All right. I'll move fast.

So, this is what an audit log looks like, and this shows on this date, at this time, this field name was accessed for this policy, this version, and for this purpose, and whether or not that consent was conformant.

So, this is the first enterprise privacy management system available that actually shows what people do with data in your organization and whether or not access is compliant with the privacy policy that's been digitized.

A lot of our customers who are deploying this are realizing some significant benefits, and it goes to some of the ROI discussion we had earlier.

We're taking privacy management out of the enterprise infrastructure. We're putting it into middle-ware, which means that application developers don't have to think about building rules into their systems.

And because we centralizing data authorization, we're making security management simpler and more effective. Because you've got this automated auditing capability, it means that, at the end of the year, when you've got a privacy audit, you press a button, it's the George Jetson age, you press a button and out spits an audit log for everything you've done, for every customer, for every system that's been monitored for a whole year, not what you said you've done but what you've done.

This is the set of companies that we've worked with for the last two years.

We announced this product in October of last year. We've had a very collaborative, fruitful collaborative with a lot of these companies.

They've been tremendously helpful in helping us understand what their enterprise privacy challenges are, and working together with them, we feel we've brought a really interesting and mature technology to market.

So, one last comment about -- this will take 60 seconds.

About three months ago, in collaboration with W3C, we published a new privacy authorization language.

One of the things that we've discovered from working with P3P and Privacy Manager is that, while P3P is a terrific open standards-based policy declaration language, it falls short from a data authorization perspective. There are some features that some of our customers have asked us for that prompted us to go and see if we couldn't extend it, enhance it. Today we’re working very closely with W3C, and we've published a new language -- EPAL -- as an IBM research note as an example to industry and our technology colleagues about what a full-featured privacy enforcement language could look like. I'll just briefly talk about some of the features of EPAL.

P3P is a positive policy declaration language, which means you can only say what's going to be allowed. You can't say what's not. And EPAL, of course, is both a positive and negative. We have positive rights and negative rights.

P3P doesn't provide for conditions. That is, I can use this data for this purpose for the following conditions, and so we developed in some very complex built-in conditional statements which allow, say, health care organizations to determine how data is going to be used in a variety of different instances.

And then, finally, we also added something which we think is really interesting, and that's action. What can be done from an IT action perspective?

Data can be accessed for the following purposes, and it can be read, it can be copied, it can be deleted, it can be printed.

Again, we just published this a few months ago. We're doing a workshop with the W3C in Kiel, Germany, on June 20th to preview this.

Our idea is that we're going to be sharing this in forums like this around the world for a while to get industry feedback on how other folks see this language, to make sure that we get a lot of good discussion about this, because we think this is an interesting example, but we don't have all the answers, and we'd like feedback from you about how you could envision this language playing a role in your enterprise.

Finally, we're doing a lot of things on privacy management today from a technology perspective.

We have an IBM Privacy Research Institute, which has about 20 projects underway currently. Kathy Bohrer from our research group will talk about that a little bit later.

We had an Almaden Privacy Institute event a month ago, which was an academic look at privacy technologies.

We have designed Tivoli Privacy Manager.

We have, as I said, this Privacy Council and this Kiel workshop coming up.

Questions later.

Thank you.

MR. SILVER: Thanks very much, Steven.

Let's talk now about threats that businesses face to their systems, both internal and external, and we have Christopher Klaus here to speak about that.

MR. KLAUS: Thanks.

Good afternoon.

We look at privacy from the perspective of security, where security has three main goals: confidentiality, integrity, and availability. And probably the two goals that overlap a lot with privacy are confidentiality and integrity.

The layers of data, application, infrastructure, and network are good areas where, if you don't have good confidentiality or integrity built into the systems, there's no way you can have privacy. I think Christine said that the Internet has a lot of vulnerabilities today, and to that extent, by default, the privacy we see implemented in a lot of organizations is easily compromised due to just exploiting confidentiality vulnerabilities.

One of the reasons why we see that is one of the current methods of trying to protect computers and their operating systems and so on is through security patching.

Anybody do security patching here? Is there anybody who goes out and applies all their security patches?

We've got two people. All right.

So, there's one guy who doesn't have to patch. There's a lot of people who don't patch.

But the reality is we find that most companies we look at don't patch either. So, you aren't alone.

And in fact, we find that when they do attempt to do security patching, there are a lot of issues with security patching, especially in a production environment, where you're trying to do business and share your private information between organizations, et cetera. Re-booting your production servers on a very frequent basis is extremely hard. When you look at all the problems with, as we've talked about, some custom or legacy applications and operating systems, sometimes you can't apply the security patches.

When you do apply the security patches, they break the applications.

So, there are a lot of difficulties for organizations to really roll out security patches consistently and aggressively across all their systems and applications.

A good example of how vulnerable the Internet was in terms of databases -- recently, I think in February, you had the Microsoft Sequel slammer worm that spread across the Internet, infecting databases. It brought down a lot of ATM's. I think in Korea a lot of their ISP's were brought down.

But what was interesting about that event is this program infected these computers and actually had all the access to the data that it wanted, but the payload or what the program actually did was just infect the database and then start to try and propagate the worm from that machine to other machines.

The author of that worm was not very malicious. They did not delete the data or change the data or copy the data to other places, but the potential risk there is significant.

Everybody who got infected -- all those databases that were exploited by that worm -- anybody manually could have hacked into those databases, as well, and had access to the data and done more malicious activity out there.

So, that's one example that's very visible, that a lot of people saw on the Internet.

We deal with a lot of organizations, especially financial institutions and retail, where they're getting targeted for more malicious attacks or someone tries to break in, download the database of consumers, and do identity theft. So far, in most situations, if the company can, they bring in an emergency response team and they try to deal with the incident as a one-off. But in most cases, the information that the company got hacked never actually gets back to the consumer. In California they just passed a law that says if you get hacked and the information of consumers was compromised, you need to report it.

But most other states, almost all the other states, none of them have any laws to actually cause a company to report that they've been hacked and that you're potentially at risk. For a lot of banks, it's actually a lot cheaper to just charge-off consumers that have experienced identity theft on an ongoing basis.

So, rather than compromise the brand and have to change, you know, 100,000 credit cards and all that, it's just cheaper to hide the fact that they got compromised.

We see that as a problem, long-term, for the industry.

Some of the security tools that I think are going to come out or are in the process of coming out within the security industry to help deal with confidentiality, integrity, and availability -- one concept is virtual patching.

Basically, virtual patching is a simple concept where you have protection agents that are deployed on the network, on the servers, on the desk-tops, lap-tops, throughout the infrastructure, down to smart phones. The protection agent analyzes all the traffic for attack patterns, all the techniques that hackers use to break into systems or all the techniques that worms and viruses are using to break into those systems, and if it sees those attacks, actually stops them.

So, what you actually do is you're stopping the risk, stopping the vulnerability and threat without actually changing the operating system or changing the application. This has the same effect as if you had applied a security patch.

Now, the advantage is this is a much more effective way of applying virtual patches where you're not re-booting the servers every time you want to stop the latest threats.

You're basically updating your security intelligence -- what traffic patterns are bad. Just like anti-virus programs update looking for new bad files, this thing is looking at traffic and stopping those attacks. Therefore, you can reduce a lot of that risk without actually having to re-do your custom application to apply this virtual patch.

There is some talk about having defense-in-depth. It has to be thought at from a network server, desk-top level. It's got to be in-depth.

One of the things that was pointed out was firewalls as being the standard technology that people are using to protect their corporate assets. Almost every Fortune 1000 company that we've dealt with has so many firewalls with so many rules, with so many partners, et cetera, that those firewalls are turning into basically routers, meaning that you've opened up your access to so many other areas that the concept of having a boundary protected by a firewall is slowly going away in terms of being a good protection device.

I think over the next year or so, we're going to see more protection capability put into that protection gateway to actually look for attacks regardless of what the rules are, because right now most firewalls allow you to have all kinds of data going through. The problem is on certain rules -- like Port 80 is a common web port, right? And you have instant messaging going through those ports.

Right now, most firewall admin's can't stop certain applications, for example, somebody mentioned stealing music earlier.

Well, P-to-P applications like Kazaa and Yahoo Messenger and other chat programs all go and try to evade the firewall, right? And therefore, one of the challenges is can we stop those applications if you have a policy against it? One way to do that is to get down to the application level, look for either protocols that are considered dangerous or look for threat patterns or vulnerability patterns and stop them at those levels.

One of the things we're going to see is probably a more pervasive protection system throughout more organizations. Because it's easily update-able, it becomes an auto-immune system.

We constantly are updating the security intelligence, so you're fending off the latest attacks.

As we move to a zero-day protection goal, if you think about all the attacks that are out there, the majority of them -- especially worms -- happen within the first day, within the first few minutes, actually.

Like Sequel slammer -- it took 15 minutes for it to spread across the Internet.

It used to be longer; for example, the I Love You virus took seven days. You could track it from Asia to Europe to the U.S.

We don't have that luxury anymore. So, we've got to move to a much more efficient and more effective model of protection out there.

The other thing that we're seeing as a security trend in large companies and small is there has been a focus for the last 10 years on point security products and saying, I have a problem like viruses, let me go get anti-virus protection; I have a problem with intruders, let me go get intrusion detection; I have a problem with denial of service attacks, let me go get a D-DOS package. You ended up with a lot of point products out there that weren't working together cohesively.

What we're starting to see now is that security is moving from a mind-set of solving it with technologies to more of a business problem.

Security has been escalated to such an essential state that now it's high enough in the organization that you have business people asking how do I do security in a more effective manner. One of the effective methods is to provide a security platform or framework for bringing together all these different disparate products under a common policy, just like you are doing for privacy statements.

There needs to be security statements that are common across organizations, common across all security products, so that there is a consistency, as well as being able to check, hey, I'm about to connect to a partner, what's their security level vis a vis what's my security level.

We see that happening, and I think what you're going to see -- I've got one minute, and one thing I wanted to point out about the way we're doing security today. Imagine you went home and you got a really good burglar alarm system for your front door and then you got a different burglar alarm system for your side door and another burglar alarm system for each and every window, so that when you walked into your house, you had to have a different PIN code and you had to run around your house to every access panel and turn off the alarm so that it didn't go off. Then if you had to leave, you had to go turn them all back on.

And if you ever had an actual burglar break in, you'd have different alarm codes, different error codes. It would be extremely hard to understand what the heck was happening in your house.

But that's how businesses are deploying security today. It is very inconsistent, mostly not centrally managed.

One of the problems is organizational structure. You have different groups responsible for different components, and therefore, everybody's picking their own burglar alarm system. They haven't thought about the broader picture of how to make all these things work together.

We see in the future moving towards an integrated platform security view around organizations.

I think, on the earlier model where you're a mom-and-pop business or a small, medium-size business, a lot of these technologies today are probably too complex to use. I'd be surprised if a start-up is really using DB2 and Oracle and other technologies today.

It's just so hard to do a lot of these

enterprise applications.

We think, long term, at least from a security point of view, we're going to see more and more of a managed protection service, where you don't have the expertise, but you let the ISP, or whomever you're getting your band width from, come in and quickly apply some security technologies. They can either provide a gateway protection and/or protection down to the servers and the desk-tops and potentially lap-tops, so you can have somebody else managing that on an ongoing basis for a low monthly fee.

I think that's going to be the direction security has to take over the next two or three years to be able to offer pervasive security everywhere. It's just too expensive, and the expertise out there to do good security is very small.

There are not that many security experts, and in fact, very few schools are giving security degrees. It's growing, but security it's not so critical that it's part of every engineer’s degree.

There are a lot of challenges that we're overcoming, but we're getting there.

At a high level, that's the vision of where we need to go with a pervasive platform for security. That will help ensure your privacy, because no matter how good your privacy statement is, no matter how well you design your system, if it's built with a lot of cracks in the foundation, it's very easy for any hacker or any malicious worm to bypass those systems and compromise the data, and that's where we need to focus on from a security point of view.

MR. SILVER: Thanks very much, Chris.

Websites these days are a host of very complicated information flows. Let me ask Michael Weider how privacy officers can ensure compliance. Are there any tools available to assist them in that?

MR. WEIDER: Sure.

Steven talked about the back-end side of your systems. Once you collect data from your customers, what are you doing with it internally?

What I'm going to talk about is more about the front end of the website, which is where you have these pages on your site. There may be hundreds or even thousands of pages all around your website.

How are your privacy policies reflected in the development of those pages, and are they being complied with internally?

If you look at this challenge, it's really that the chief privacy officer or legal person creates a policy on the site.

You have web developers and marketing people creating the web content itself.

How do you ensure that the pages and sites that are being created accurately reflect the policies that the company has?

In many cases, this is a very difficult challenge, because there may be thousands and thousands of pages on the site. They may be changing every single day. There may hundreds of people actually creating this content within a large enterprise. You may have out-sourced some of it to third parties.

Getting a handle on how to ensure that your website is appropriately reflecting your privacy policies is a difficult thing.

For example, where are all the points where we are collecting sensitive or personal identifiable information on our website? Are we collecting that data securely? Is there a privacy statement at the point of collection providing proper notice? What sort of tracking technologies exist on the website that some marketing people might have put on there that are tracking the flows or potentially exchanging data with third parties on the site?

The challenge for someone in the privacy field is that they have accountability for ensuring that their company complies with the privacy policies, but yet, they have very little control or insight as to what is actually happening within the website itself, which is really developed by all these web developers and the like around your company.

If you look at what are your options, then, in terms of how to address this sort of challenge, there are a couple of things people are doing.

One is nothing. This happens a lot, that people really aren't addressing this issue at all.

The second is that sometimes they do spot checks -- they review the privacy policies when a site is first launched.

The people sit down with legal and they say -- here's what we're doing in the site, is this okay; okay, we're going to review all this. The problem is obviously that the site today is going to be very different than it will be tomorrow.

The third option is to do spot checks and to manually go through the website, looking at where there may be issues on the site and trolling through the pages, clicking on all these links and finding all the places we're collecting sensitive information, making sure it's being done correctly.

Again, the challenge there is that the site is so big that the manual effort and the rate of change makes this very ineffective and really uneconomical, as well.

So, what are the tools that exist today? Our company, Watchfire, developed a product called Privacy XM. Essentially, we’re trying to automate that process. If I sent you out on the website to go and look at all these points of collection and the privacy policies and so forth, I’d want to know how is that represented in the content of the site?

What we're trying to do is send a software program to automate that process. Essentially, the way it works is that you define your privacy policies in the form of rules to the software. The software then recursively scrolls through all your content.

Maybe you have about 100,000 pages on your site. We'll go through that every single day, and we'll examine all those points where you're potentially collecting data and tracking people on the site and come back and compare that against the policy and then flag issues that exist that need to be remediated.

What the tools can help you accomplish is to, one, automate some of that process of the compliance process. As Larry mentioned this morning, a lot of companies have a privacy policy on their websites, but there are very few companies that are actually going through the compliance and the monitoring of their policy and practices to ensure that they're actually doing what they say they do.

The other thing that the technology can assist with is that sometimes you may be doing what you say you're doing, but it may be the omission in your privacy statements or your policies that is the problem.

For example, if someone in marketing has introduced some new whiz-bang tracking technology that profiles the users and sees where they're going and so on, but yet it's not covered in your privacy policy, that may be an issue for you that you want to make sure it is properly represented in your policy. In a worst case, you say you don't do that in your policy but you actually are doing that on the site, which we see happening a lot.

The age old problem is how to bridge the alignment between the technology developers and the business problem. This type of technology can help in that process in that, one, it can give the CPO more insight as to what is actually happening in the website, give them reports, give them dashboards, give them data as to how privacy is being represented across a site.

And secondly, maybe even more importantly, it serves as a vehicle to educate a lot of these diverse and disparate web development groups that you may have inside larger company as to what they may be doing wrong, because in many of the cases, it's really the lack of training and awareness and the lack of knowledge that they have done something wrong rather than the purposeful violation of a rule. Software can troll through websites on a recursive basis and then push out a report to managers and also to the developers of the sites that tells them, hey, you've done something over here which contravenes our rules, I need you to go fix that.

It serves as both an oversight capability for ensuring compliance but also as an education vehicle to people to tell them what they're doing wrong.

There are two areas where this technology is being used on websites.

One is on the live production site, which is that you want to monitor your live sites that customers are seeing to ensure there's nothing on there that we don't want to be on there, and if it is, I want to know about it fast, before someone else does.

The second area where we're working with a lot of customers now is in the area of prevention, which is to say I don't want to be bailing water out of this boat all the time. I want to plug the leak, so that we find out where these privacy issues are getting in and try and build in compliance into the web publishing process.

What we do there is take the technology and embed it into the customer's web development publishing process. If I create a page, I submit it to my system to be posted to the website, It's then passed to the technology group and evaluated against these rules that we've defined ahead of time, and then it automatically comes back to Mike and says no, your page has been rejected, because you've done something over here which is against the rules or, no problem, it's accepted and it passes on to the next stage.

What I've seen in traveling around and talking with customers about this issue is that there are a lot of sites out there where people think they're doing one thing and they're actually doing the other.

When you actually dig into how do you help them with that, it really is about making it easier, making it more automated, making it part of people's processes in that people are moving fast on the web, they're trying to develop content, there are fewer resources today than there were a couple of years ago to do this. What you need to do is figure out a way to make this a lot more economical and a lot easier for people to comply with the privacy policies that you have. We really see that as embedding this type of compliance technologies and automating this review as much as possible into your publishing process. Instead of asking people to go out of their way, just make it part of the flow that they already have.

MR. SILVER: Thanks very much, Michael.

Ari Schwartz, we've heard about quite a tool kit here. Do you have any comments from your perspective?

MR. SCHWARTZ: Well, a lot of what I had to say was taken up and was said in the first panel and earlier in this panel, so I have the advantage of being able to be pretty brief here.

One point that's been made over and over again today, and Joe and Gary both it in the first panel, and Joe again in this panel, is that essential to being able to go about finding privacy is being able to track the data flow and understand the data flow, and all of the tools that we've heard about do that to some degree.

You can break down understanding the data flows into two different sets. I was doing this as I was listening to people just now.

The first, understanding and authorizing data flows, more of the later ones that we heard about, what Steve is doing, what Michael's doing, what Joe talked about to some degree, the idea of being able to understand and figure out what goes on internally within the organization is a positive for privacy.

There's not really a question there. It's something that we need to do, as we were talking about in the first panel.

To get even the basic grasp of privacy controls, privacy policies, you have to be able to understand the data flows. These are tools that help to do that.

I think Steve Adler's announcement about taking P3P to the next step, using it behind the scenes in databases, and coming up with a vocabulary is a positive development, as well. It's something that people who have been promoting P3P use have seen coming down the road for a long time, and vocabularies are essential to making that happen.

I think we're very optimistic about where that idea is heading. We'll have to see how it develops over time.

The second set of tools are those that are aimed at securing or improving internal and external data flows, what Joe was talking about, what Christine presented for Liberty and what Robert talked about for LeGrand, and that's the more difficult area of privacy protection, because it really is about the internal and external data flows, and Joe talked about the peanut M&M.

If you're talking about the peanut M&M, the difficulty is in the internal flows of the information but it becomes more difficult when you start going external and people are using different types of systems. Some of these tools are trying to get at making that a little bit easier for the information to flow.

While doing that makes information flow, it can tend to detract from privacy. We're trying to come up with some ways to protect privacy from the beginning in this discussion.

I'm going to summarize what we've heard already on this panel.

Liberty is non-proprietary. It's decentralized. It's got best practices, which are very consistent with what the principles of the Authentication Privacy Principles Working Group that we put together has said on these issues. That's very positive.

LeGrande, asking the OEM's to set opt-in's and is user controlled; again, these are two very positive things.

The more difficult side is that the proof of whether these are going to be privacy positives, comes down to the implementation. We can hear all we want from Intel about the way that the technology is being created and what they say the best practices should be, and what Liberty says the best practices should be.

When we actually see the software that the companies are actually going to use and the controls that they're going to set and the options that they're going to give to consumers out there, that's a whole different story.

So, while we're very positive that we've been hearing the right things, the question comes down to is there going to be this diversity of services out there so that individuals really do have the kind of controls that both Robert and Christine hope that they will have down the road.

I think it's still too early to tell that, but I hope to hear maybe from Craig what they're doing in this area, because again, the consumer-facing companies really have to step up and provide the wide range of privacy protections and controls that we've heard about discussed in the abstract today.

MR. SILVER: Thanks, Ari.

Why don't we go ahead and go to Craig and hear about the perspective of a single company engaged in a consumer-facing business?

MR. LOWERY: Well, one of the things to consider about a company like Dell is what drives our business, and that's customer demand.

We're looking to customers to come to us and say this is what we're looking for in a product from Dell. More and more, of course, we're seeing security and privacy as chief concerns that our customers have, among other things, like low cost and quality, which are always driving us to deliver products to market.

As a technology vendor, Dell is committed to delivering value through reducing cost, and that's for acquiring products, deploying them, making sure they're inter-operational, and also maintaining and managing them once you've bought them from us.

We believe that these benefits are best achieved through consensus, and that would be through standards. We're very pro-standards.

Hearing all of the talk today on the panel about standards is very positive and is something that Dell is very much behind.

Anything that's standardized, we believe is good for the customer, because it drives costs lower, and it makes things more inter-operable.

Everybody understands how it works, and it's not a mystery anymore.

Right now, security and privacy is so mysterious, you know. How do these things work? How does information get encrypted? What does that mean? And what does it mean when encryption gets broken?

Consumers are very confused by these concepts. We've got to make this simpler for them, so they understand what to ask us for.

Once they start asking us for those things, it's much easier for a company like Dell to justify bringing something to market.

That's just to give you an insight into how our company works, and if you want us to bring something to market, get customers asking us for that. We'll jump.

As these technologies mature and customers are asking for them, we'll leverage the benefit of our direct model, which means we take orders directly from our customers and we deliver directly to our customers, to deliver those technologies to market quickly and affordably.

Securing the enterprise is only possible through partnership, though. It's not something that a company like Dell or our partners like Intel or Microsoft can do on our own or even if we three go off in a closet and talk about it for a while.

It's going to require that those who are deploying these products have an understanding of their responsibility to create a secure infrastructure.

Dell is placing more and more emphasis on security as a chief design consideration. I think that's an obvious thing that all of us in the industry are doing at this time. Certainly, as a hardware vendor, we're acutely aware of physical security. On the first panel, there was a little bit of laughter about the notebook lock, but let's not forget that those things are very important.

Physical security is the basis on which all other security is going to be built upon, and when you start looking at things like platform authentication, the trusted platform module, for example, that's an example of something that's rooted in physical security.

If that box is not physically secure, it doesn't really matter if the TPM that's down on the mother board is telling you or attesting that this platform has not been compromised.

Physical security is where it begins. We've got the things like chassis locks, intrusion detection, drive carrier locks, rack locks, all those things you expect. We're going to continue to deliver those, and we're going to continue to look for ways to improve upon physical security, because we are chiefly a hardware vendor -- but I don't want you to box us in to just being only a hardware vendor, but primarily as a hardware vendor, physical security of hardware is going to be something that we're going to focus on quite heavily.

Another example of creating even more security software configurations is a new Dell offering that's available through our custom factory installation unit. Dell is beginning to offer desk-top systems installed with Microsoft Windows 2000 preset to the Center for Internet Security’s level one benchmark.

I'm sure many of you are familiar with the CIS and its work on level one benchmarking.

This is a separate offering from our normal Windows 2000 installation. You can still get the default install. That's going to continue to be available.

Let me tell you something about the CIS level one. Later this afternoon, in another panel, the Center for Internet Security will be here and probably will address this in more detail, but the level one benchmark is a consensus of the current best least restrictive security settings for Windows 2000.

They have benchmarks for many operating systems and many network devices. We have focused on Windows 2000 as our first foray into this area, because we have customers asking us for that.

These settings were developed with input from government agencies, business, universities, and individual security experts.

In providing the factory-installed benchmark systems, Dell is responding to customer demand for a hardened operating system direct from our factory, and although we're targeting this at our public sector customers like state and local government, I think anyone who’s looking for a certain level of security such as that defined by the CIS level one benchmark can benefit from purchasing a system from Dell that comes preset with these configurations.

It saves them the trouble of having to download the benchmark from CIS, go through it, understand how to set registry settings and all of that kind of thing, which, frankly, should not be a burden that we place on people that are receiving systems from us.

So I think this is a great added value to our customers, and we're looking forward to seeing how this product is received.

It may even give us impetus going forward in the future to look at other platforms that we could release with benchmark settings.

As I said, it depends on customer demand. If customers come to us asking for those things, we certainly look into them, because we want to meet their expectations and deliver products that can help them.

In other areas, there are things that you are expecting from us, things like system bios, passwords, and other robust forms of authentication. We now have smart card readers that come as a standard, built-in feature of our Latitude D series notebooks. If you look at desk-top systems, we can do smart card readers now on a keyboard that comes with the system.

We’re looking at those types of smart card-based authentication, because we have customers asking for them, particularly in vertical markets like the financials and health care. That's where it's getting a lot of traction right now, but we expect to see that increase in the future.

We also are able, through our direct model, to offer third-party solutions directly to our customers through our software and peripherals unit.

We look at products that meet our customers' demanding standards and make those available for purchase online.

We're a one-stop shopping place. We like to make things easy for our customers to get what they need when they come and shop at Dell.

We also have telephone support, access to our website, and technical support at a premium level for customers who are looking for help in deploying the products that they purchase from us. That's Dell Professional Services, for example, where you as a customer can order from us.

I'd like to deploy this server, and I'd like for it to do this particular thing.

Built into that service package when you buy it from Dell are all kinds of different considerations, including those for deploying a secure system.

Service offerings can help customers who don't have security expertise. They can purchase that expertise from a company like Dell, and our professional services people can bring that in.

On the engineering side, we're involved with The SANS Institute, doing SANS training, and going to SANS conferences, because I think The SANS Institute is one of the premier institutes for disseminating information.

Our engineers are getting that information. They're starting to think about security as they code software, for example.

We're, of course, in contact with the CERT Coordination Center, watching vulnerabilities when they pop up, working with the Center for Internet Security, as I mentioned, and also the Free Standards Group for standards around security.

As I said, we're very pro-standards.

We're making available pre-packaged and customized services, which I mentioned. If I wanted to leave you with anything, it would be the last paragraph here I'd have in my thoughts as I was collecting them before coming here today, and that is Dell is a security aware and a privacy aware company.

We know it's important to our customers, because we're hearing it from them. They tell us.

You're all interacting with your customers, too, and I know they're telling you security and privacy are becoming even more important concerns for us. It's not knowing about it, the uncertainty about it that's causing a little bit of trepidation for them when they buy into technology.

So, what we have to do is make it easier for them to understand what they're getting when they buy technology that's security-related, and we have to help them to deploy that and then be there for them when they need help in servicing it.

We're doing it in a way that's consistent with our model, our direct model. That's what drives everything. Our goals are quality, low cost, easily integrated standards-based solutions that meet our customer requirements that we deliver directly to them.

Thank you.

MR. SILVER: Thanks very much, Craig.

Let me ask some questions of Gary Clayton.

First of all, to what extent are these tools being used, and how are they deployed among businesses? Also, what are small businesses to do with regard to these concerns?

MR. CLAYTON: I might just tell you something. We're talking about all these wonderful solutions and wonderful technology. Yesterday I was out at a company that is a small, 60-person technology company. It processes about 60 million transactions a day, and they were showing me biometrics and security processes and cameras and everything else. I happened to walk out of the conference room where we were meeting, and they had a little wooden wedge by the door, and I asked what that was for. They used it to prop the door open for people.

And I make the point -- we've got all these solutions that have to be deployed in organizations where people are going to use the wooden wedge of their choice to get things done.

People are people, and they just don't understand what's going on.

We have worked with a lot of large companies that are using bits and pieces, if not many of the types of solutions that we're looking at here. You may get the impression from looking at or hearing today that all businesses need big or complicated or even expensive or inexpensive solutions. They need parts and pieces of all of them.

What I've seen since 9/11 is, amazingly, an increase in the issue of security clearly by Homeland Security, but in the last year, a real emphasis on making privacy and security an integral part of a business. You're looking for ways to do it, and it's not just big businesses doing that. There are starting to be smaller organizations doing it.

We talked about technical solutions primarily here, or tools.

The other side of that is awareness and training, about why you don't use the wooden wedge, why you need to have tools.

There are tools that are being deployed that you have to really think about -- I think Michael made this point -- how do you tie it into what you're actually doing. For a small business, the challenge is how do you document, how do you find tools that train you, how do you find tools that, when you're designing a website or you're doing any of the steps that we've talked about today, you understand how it impacts your business.

I don't think most companies have solutions. As you made the comment about Dell, what really needs to happen and is not certainly happening is the public demand for these kinds of solutions is nascent. It is just growing. And small businesses, particularly, need to look for solutions that are affordable, but more than that, solutions that translate themselves among different silos.

We talked about this in the first session this morning -- and as you say, people were going what the heck is XML or what's a cookie? I mean there were acronyms heard today -- and I work in privacy and security -- that I didn't understand.

We've got to get away from that and have tools that provide functional solutions.

I think those are just beginning. They're coming up with some wonderful things, including with business alliances doing it. We're working, for example, with BBB OnLine to come up with some online training tools that will be used by a large number of people, particularly small and mid-sized businesses, that can help them understand why this is important.

But I would think if you were asking how much it's being deployed, the market is just beginning. I would say that if you ask any of these companies, it's a small portion of any of their business to really sell these kinds of solutions.

That will grow, and I would predict over the next four to five years, it will grow primarily at the big ends, the regulated end, and the companies that do international work. But it's increasingly going to have to have an impact on the small to mid-size company, where you don't pay more than $10,000 a year for a solution. That's all they can afford.

MR. SILVER: Let me ask those from the audience who have questions to go ahead and begin lining up, and let me pose one more question to the panel as a whole about small businesses and out-sourcing, if anyone wants to take up that topic.

MR. ALHADEFF: I think Michael addressed having managed solutions of some kind out there. Actually, you may have addressed the concept of an ISP.

You also have companies that do full-end data management, whether it's Oracle, IBM, EDS, a number of companies offer such expertise where you get a lot of the management expertise at a price that's more commensurate with what it is that you're using, with a growth strategy that, as you grow and develop, you can either eventually take it in-house yourself or you can continue to out source.

I mean GO was a great example, because the technical guys they have could never manage the portals or anything else that we were talking about. So, either they had to develop the technology infrastructure or they had to out-source that expertise.

They came to a point where they had two choices. Early on, for a small company, the out-sourcing choice may be somewhat more affordable, but that doesn't mean that you don't have to put all the solutions in place and develop policies of some kind or another, as well. The back end is still the back end, and it's got to meet with the front end, and it's got to understand needs and requirements. While someone may be able to give you a template of a solution, you still have to customize it for your needs.

MR. ADLER: I would phrase it this way. What is an enterprise today?

We can't look at enterprise computing any longer from the perimeter wall and everything inside. It's a value chain. And where it starts and where it ends between third parties that provide discrete services across so many different boundaries, functional organizations, that the out-sourcing environment already exists, in a sense, between all these different groups that are providing these services, whether it's out-sourced HR or it's printing or it's security services.

That value chain for most enterprises around the world already -- it's part of what Liberty was talking about earlier, this virtual enterprise that we have today, and the privacy and security framework between all those organizations, beyond just what today exists as a contractual obligation. I have a contract with another company that says they have to protect my data, but I don't have any assurance that the contract in any way is being maintained. If I get taken to court, I can always hold up the contract and say, well, they were supposed to.

That's where the complexity of the challenge is today.

I agree with what Gary was saying earlier. We're at the dawn. We're at the starting point of exploring real enterprise security and privacy technologies that integrate into that value chain, and we're at the dawn.

We're at the beginning of discovering how we can take these ideas that we've all articulated today and start building them into this value chain so that they do become transparent, something we can take advantage of, we can take for granted that it exists, and we're just at the beginning of exploring how to do that.

MR. SILVER: Thanks, Steven.

We'll take the first question, please.

QUESTION: David Weitzel, Mitretek Corp. I'd like to direct this question to Ari Schwartz and Christine Varney.

We started off this morning with having a government representative who's worried critically about privacy in the government space. In an FTC conference, it surely makes sense to concentrate on consumers. But it's about citizens, and one might consider that citizens don't have choice and have greater rights or should have greater expectations than they do in the consumer world.

What should we expect in a town here that's doing all kinds of stuff about e-gov to worry about the security and privacy issues as we look at government-based systems?

MR. SCHWARTZ: It's a good question.

David has actually worked on the authentication privacy principle with us, so he knows that we separated this out into two sections, the consumer-initiated transactions and government services. The government services piece is actually, in some ways, more difficult to write.

How much control can you give an individual as an agency when another body might make a decision about what happened to that information further on down the road that you have no control over as a person trying to deliver this service.

So, there is a catch and it rests on what kind of rights individuals have in the law.

We could go into great detail about how this works in the Federal Government today, in particular, because of the Privacy Act and the way that the Privacy Act was written 25 years ago. The whole structure has changed over time of how information is collected and how it's stored and how it's used.

So, it's become out of date and does not give those kind of protections that we need today.

Some states are trying to look at some of those issues, but the Federal Government has a larger question in terms of building these kind of protections in for just regular services. I'm not even talking about data mining issues, which is a whole other set of issues that fits in there.

MS. VARNEY: Well, I think that was a great question, David, and you know, the fundamental question, what expectations should citizens have if their government delivers them services regarding privacy, and the answer is the highest.

There should be no higher level of privacy anywhere than in government-delivered services. In this country, we have a very long tradition of regulating what data government can collect, what they can do with it, what the citizens' rights are regarding that data, far more so than we've ever had in the commercial side.

So, I would expect that as we make services easier for citizens to access, we are going to be able to strengthen the kind of privacy that we as a government provide to our citizens.

Because we now have the ability to vastly streamline and ease the ability to collect and exchange data between the government and the citizenry, doesn't change in any way the fundamental historical and legal tradition and obligations that we have undertaken as a government.

If anything, it makes it easier to safeguard the privacy of our citizens. I would hope all of us will aggressively watch and advocate that that will, indeed, happen.

MR. SCHWARTZ: Let me just pick up on the last point, which is that the E-gov Act of 2002 actually went into effect in April requiring government agencies to have privacy impact assessments for new technologies that the information on more than 10 people. That is one positive step that we've seen.

The rules regarding the assessments are supposed to come out sometime this month. Hopefully that will mean that there's implementation and will be a marketplace for some of the tools that we're hearing about here inside government agencies.

MR. CLAYTON: It might also be as part of the business case that agencies have to make in getting new systems and developing technologies. They now have to write into the business case very detailed information about privacy and security and show alternatives considered. It's basically the same thing that we've all talked about, both this morning and now, build a business case, go through it, look at the options, talk about solutions, and come up with something that's cost-effective to deliver what you've promised. But that sort of analysis and planning wasn't there just a few years ago, and it's very encouraging to see it happening now.

MR. SILVER: We'll take one more question and I'll ask the others to perhaps approach the panelists later if they're able to.

QUESTION: I'm concerned about Mr. Lowery's example.

I certainly applaud all those things that Dell, Compaq, IBM, and others are doing to add features. I'm applauding the PC hardware vendors for adding security features that consumers may opt to have, like Windows 2000 or some of the TPM features.

I'm a little concerned about that, and I've got three examples.

When I go and fly on a plane, I don't concern myself with the adequacy of the air traffic control system, although I've heard it's pretty antiquated and needs a lot of help.

MS. VARNEY: Yeah, you probably should.

QUESTION: When I buy a new car, I don't ask Honda whether there's a firewall, because I know there's a firewall between the engine and the passenger compartment. It's there. The government requires it, I assume, so it’s there.

And the third example is when my mom goes to use the firewall that I put on her PC, it's a little anti-climatic, because I've told her about this great firewall software and I install it and I configure it so it doesn't nag her, and it doesn't really do anything. You know, she's bored with it.

Why did I ask her to pay 40 bucks for this software that doesn't really do anything?

My concern is that consumers sometimes don't know enough to ask for the baseline. The baseline doesn't meet adequate standards.

The baseline in the car does. The baseline in the air traffic control system may not.

What I've done for my mom hopefully will help her, but she never would have asked for that from Dell. She never would have asked for that.

And my concern is not so much whether regulation is appropriate but how do we raise the baseline such that it does implement the common sense security best practices rather than leaving everything up to consumer choice, which in an increasingly connected world puts us all at risk.

MR. LOWERY: I think it's an evolutionary process and it's happening now.

I think, for example, what we're doing with the CIS benchmark is an example of bringing value into our product as best we can. We do the custom factory install, we have the opportunity to add some value there, and I think what you'll see is partners like Microsoft are taking steps to roll those concepts back into their product so that we have to do that.

It's a learning process. It's partnerships, sharing information, disseminating information through organizations like SANS.

As we said, it's the beginning of understanding how important this is and crucial it is, because we've become so dependent on these systems so quickly. Now we understand the other side of the issue, that they have to be secure and they have to guard our privacy.

I do understand that many consumers don't want to take the time to understand, because they shouldn't have to. It should be baked in, and they shouldn't have to worry about those things, and I think all of us in this industry want to get to that point. That certainly is the goal. What we're doing now is part of what's on the path of getting from where we are now to where we want to be.

So, as long as I continue to see us making progress, I think we're addressing your concerns.

MR. SILVER: Steven Adler has the last word.

MR. ADLER: I would totally agree. I would say that in the real world, we all have a mental model of security and privacy in our homes. We know when we can leave our doors open, we know when we have to lock them at night, and we understand the technology that we have around us to keep ourselves secure and what information we should share. All of us on this panel are trying to work, oftentimes, together to bring technology to that same simplistic level, so that your mom doesn't have to worry about the firewall. She can take it for granted.

It's part of the transparent system that supports doing business in an electronic world.

MR. SILVER: Panel three begins at 1:30. Please be back for that, and join me in thanking our panelists. They've been brilliant.

(Applause.)

(Whereupon, at 12:45 p.m., a luncheon recess was taken.)

AFTERNOON SESSION

PANEL 3: Current and Emerging Frameworks for Protecting Consumer Information

MS. GARRISON: We appreciate your coming back so promptly. We’re sorry we're running just a few minutes late to catch the stragglers.

Once again, I'm Loretta Garrison from the Federal Trade Commission. I'm joined today by James Silver, and we'll be managing panel three.

We're delighted that so many of you could join us for this second half of a two-day workshop on technology for protecting consumer information. We opened our discussions this morning on the business experience, engaging our panelists in some role-playing around a hypothetical business consultant situation. Our equity actors were charged with devising a business plan, then to advise a confederation of retirement communities on privacy and security issues raised by implementing certain technology services for their seniors in their communities. We hope that the issues that were raised in that discussion continue to be amplified as we go through the day.

We also learned about many technological tools that are available to help businesses protect consumers' personal information and we'll be talking more about that