FEDERAL TRADE COMMISSION

PUBLIC WORKSHOP:
TECHNOLOGIES FOR PROTECTING PERSONAL INFORMATION:
THE BUSINESS EXPERIENCE

Wednesday, June 4, 2003

8:30 a.m.

Conference Center
601 New Jersey Avenue, N.W.
Washington, D.C.

FEDERAL TRADE COMMISSION

INDEX

P R O C E E D I N G S

MS. LEVIN: I hope all of you have had a chance to enjoy some of the delicious refreshments out front. They were provided by some terrific companies -- Comcast, Ernst & Young, Internet Security Systems, Microsoft, The SANS Institute, and Trustee -- and we thank them for providing them to us today.

Good morning, and welcome to the second session of the Federal Trade Commission's public workshop, Technologies for Protecting Personal Information: The Business Experience.

Some of you were here a few weeks ago at our consumer experience workshop. We learned an awful lot through that workshop, and I'm sure we will also learn a great deal today.

It's been my pleasure to work with Loretta Garrison and James Silver and Jessica Rich, our assistant director, to prepare for these workshops.

We look forward to having our panelists share their expertise and insights with all of you today.

Before we begin, I have just a few housekeeping announcements.

First, in the unlikely event of an emergency, we will be given specific instructions by our building security officer. So, I ask you please to wait for those instructions, even though you might instinctively dash for the exits.

Secondly, please wear your badges throughout the day while attending the workshop, because if you take them off, you'll have to go through security again. If you do leave the building, you will still have to come back in through security, even though you have your badges, but we ask you please to keep them on.

And now, if you haven't already done so, please turn off your cell phone, the ubiquitous technology in the room today.

It's my pleasure now to introduce Commissioner Orson Swindle of the Federal Trade Commission.

(Applause.)

COMMISSIONER SWINDLE: Thank you, Toby.

I'm from a small town in south Georgia, and I'm a Methodist. We used to note that every time we went to the Baptist church that the real skinflints in the Baptist congregation always sat in the outlier seats and in the back, because at the Baptist church, it's absolutely habitual, they do ask for money.

Now, we are going to pass the plate here later on this afternoon, and during the next break. If I could encourage everybody to move inward as much as we can. I realize we're just about full here in the middle, and that's great, but come on in. I think it helps the speakers, and I think you would be able to enjoy it a little bit more.

Speaking of being from south Georgia, it's very hot in south Georgia and dry during the summer. I have good news and bad news. The good news is the rain's going to stop, and the bad news is that is reported to be in September. It reminds me of when I first moved to Hawaii.

I married my wife in December of '89, and I moved to Hawaii. January and February are the rainy months in Hawaii. Having grown up in south Georgia, a little town where we would have the occasional rain shower, it was our challenge as kids to know whose front porch we could run to to hop in.

We'd sprint home from school and hide from the rain and get under the trees -- this is one of those habits you pick up as a kid. When I got to Hawaii, we lived about eight or 10 blocks away from a place where we had our car fixed. I took the car down one morning right after I'd gotten there, and as I'm walking back, it starts raining, and I immediately revert to the Camilla, Georgia, strategy of keeping dry. I'm running from door stoop to door stoop and finding a tree and hiding, and after I get about halfway home, I look around and not another soul is doing this.

I mean in Hawaii, it's natural that it would rain. So, from the look of things the past couple of months, we're going to have to adopt the Hawaii philosophy and just ignore it and walk through it.

I want to welcome you today to our workshop, Technologies for Protecting Personal Information: The Business Experience. We're very pleased that you can be here and we thank you for coming and sharing this discussion with us.

Today's workshop is the second in our series that started on May 18th, when we spent the day examining the consumer experience with technology for protecting personal information.

I think we're in for a real treat today, since many of the same participants are with us again today to share their knowledge about how businesses are protecting privacy and security.

As I often say, solving problems of privacy and security and protecting the security of information systems and networks will require a new way of thinking, a culture of security.

I suggest that, to achieve the best possible results -- not the perfect results, because they don't exist, but the best possible results -- we need to keep the dialogue going.

We need all sides of the debate at the table with us.

The FTC is pleased to facilitate that dialogue, and we thank you for being active participants in our search for solutions to these very complex problems.

Shocking as it may seem, we in government do not have all the answers.

All of us -- you, the government, regulators, businesses, Congress -- we must all keep working together to promote market-based solutions as rational and effective alternatives to more and more government regulations that are too often characterized by having troublesome, unintended, and ineffective consequences on innovation. I believe this to be the best path to follow, and we really do need your help to make the journey.

I see a number of my old friends at the table up here, led by Joe Alhadeff. They're raring to go. But before I give them control of our first discussion panel, I have the pleasure of introducing Nuala O'Connor Kelly, the chief privacy officer at the Department of Homeland Security.

Before joining DHS, Nuala was the Chief Counsel for Technology in the Commerce Department. Prior to that, Nuala was the chief privacy officer for DoubleClick.

So, having a long experience working with the FTC, she knows about difficult duties. She's willingly taken on one of the toughest jobs in government, certainly in this town.

We're glad she's with us this morning to give us the view from the DHS perspective, if she can figure out exactly what DHS is.

She is a dear friend, she's a delightful person, she's beautiful, and she's up to the challenge.

Nuala, please come and enlighten us.

Thank you.

(Applause.)

MS. KELLY: Well, good morning, and thank you, Orson, for your warm welcome.

I think it's well-known that I am the chief member of the Orson Swindle fan club. I have long been one of Orson's many admirers, and I'm thrilled to be here at his request today. It's my great pleasure to be with all of you today for this important discussion of the business experience of developing and using technologies to protect personal information. I'd also like to recognize the entire FTC team which under Chairman Muris' leadership has become a leader not only in enforcement activities on security and privacy but also which, as an organization, has been a thought leader on the issues confronting both consumers and industry in cyberspace.

I've had the privilege of working with the FTC staff, as Orson mentioned, both on the opposite side of the table and also on the same side of the table, and I must confess, I much prefer to be on the same side. But either way, I'm always impressed by the depth of knowledge and the commitment that the Commission's team has brought to both of these issues of privacy and security for industry.

I'd like to thank Orson not only personally but on behalf of those of us who share in the administration's vision and goals on privacy and security, and Orson, as many of you know, has been a tireless advocate of common sense practical approaches to privacy and security.

His work in cajoling, encouraging, and even brow-beating industry when necessary -- those of us in the privacy and security community are very grateful for that work. It has served to open a dialogue between industry and consumers and enrich both public policy and industry space.

Many of you, I'm sure, know of Orson's work as an ambassador for the United States and as an emissary for America. He travels endlessly around the world to represent the United States in conversations, in negotiations, in debates over the evolution of privacy and security protocols. He's often the lone voice for the United States, and when I am lucky enough to join him, I'm always impressed by the grace and eloquence he brings to bear on behalf of the United States and her citizens.

But we should also take a moment to thank both Toby Levin and Dan Caprio for their work on this workshop and the many other conversations that have happened and continue to happen with industry and the advocacy community. We are very grateful for their work.

And I'm grateful, also, for the opportunity to talk with you this morning.

As Orson mentioned, I have a new job. Many of you know about it. It's a new job with a fairly large organization -- not a business organization but one with an important governmental mission, to protect the people and the places of our homeland. I can think of few more important tasks for the Federal Government or any federal government to engage in than to keep a country and its citizens safe.

I'm tremendously honored and humbled to be part of that mission, and as it's constantly pointed out to me by family and friends, this is almost an impossible mission -- to protect millions of people, thousands of miles of border, hundreds of airports and seaports and other ports of entry. But, as was pointed out to me recently by my boss, the mission of the Department of Homeland Security is not only to protect the people and the places of our country.

Fully central to the mission of this department is to protect the liberties and the way of life that have made this country a symbol of freedom and of opportunity for people around the world.

Both Governor Ridge and Deputy Secretary England have consistently articulated within the organization their belief that the dignity of the individual is central to our vision of successfully achieving the mission of protecting the homeland. So, while safeguarding the people and places of our country, we must also safeguard the lives and liberties, the dignity, the uniqueness, and the privacy of the individual.

The protection of privacy is neither an adjunct nor an antithesis to the mission of our department. Privacy protection is central to the core of our mission.

But homeland security cannot simply be the domain of one Federal agency, large in numbers though it may be. The defense of our homeland is a part of all of our mission as government servants, as individual citizens, and as corporate actors.

As both Commissioner Swindle and my former boss, Commerce Secretary Don Evans, have said on numerous occasions, corporate America can and should be playing a role in creating a culture of security, that it is part of everyone’s civic duty, as well as simply good management of your businesses. I will take that even a step further. We must leverage good old American ingenuity towards creating a culture of security and a culture of privacy in the development of our corporate and governmental resources, both in our technological system and in the richness of our policy debate.

And so, I ask for your partnership and your leadership as we develop together technologies that achieve whatever our missions may be, whether it's selling widgets in Wichita, providing mortgages in Montana, or securing borders near Buffalo. Let us be cognizant that building privacy and security into systems is essential, as these systems are increasingly the backbone of this country.

A recent report said that almost 90 percent of the critical infrastructures of the United States are in private hands. We need those hands to be custodians of the public trust, just as we need our government entities to uphold this public trust.

Many of you in the room represent industry sectors that deal with personal information in one form or another. Achieving good customer services, in many cases, requires, even demands that your companies know how to best serve their customers by knowing who their customers are. But good privacy and security practices further demand that you serve your customers responsibly and with respect for the sanctity of their personal data.

Similarly, achieving our mission at the Homeland Security Department will require the use of personal information about citizens and non-citizens alike. Our challenge at the department is to ensure that such data is used only in a manner that is limited, respectful, and responsible.

Having partners in the private sector who can both demonstrate and demand the responsible treatment of data, both by themselves and by their government, is essential to our successfully achieving the department's goals.

It has been said that the department is engaging in unprecedented uses of technology to achieve its mission.

This is said by people who are both happy about this and unhappy about this. As a former member of the technology sector, while I’m certainly very pleased to see technology leveraged and used and I'm increasingly confident it will be used wisely over time, the department must seek to leverage the best, the most efficient, and the most cost-effective tools to achieve our mission. The department must seek to be agile, perhaps more agile than one would ordinarily expect from a government organization of 180,000 people, but such agility is required for the war on terrorism.

And in this mission of securing our homeland with speed, with effectiveness, with agility, we must leverage the brilliance of our private sector's technological prowess. We must also learn from and leverage the private sector's awareness of the importance of both privacy and security and their willingness to embed these values into new technologies.

It is certainly an important challenge to achieve security, which we need to flourish as a country, as an economy, as a community, while simultaneously protecting the rights and the privacy of the individual. But I am confident that we will have your help in this mission, and there is more than one way to serve and to engage.

Beyond building good and secure and respectful systems that allow the country to grow and allow your enterprises to grow, we must also engage responsibly and civilly in the debate over how best to achieve security for these systems and for our country, while still protecting individual privacy.

In fact, our ability to have this free and open debate is a direct result of the freedoms which are the bedrock of our society and which we seek to protect.

Our willingness to engage in this conversation is again a sign of support and respect for our country, our colleagues, and our citizens, and I want to recognize each of you who are present today and who will participate on the various panels, people like Larry Ponemon of the Ponemon Institute -- I'm sure you'll be hearing frequently in the future about Larry's recent ground-breaking benchmark study that analyzes trust issues relating to how organizations collect, use, and maintain data.

The privacy trust survey provides information to industry and to government on the comparison of individuals' trust.

And people like Gary Clayton, whose Privacy Council has worked assiduously to create bridges and open lines of communication among government, industry, and advocacy communities.

And of course, thinkers like Marty Abrams, whose work on identity and notice and pattern analysis has been instrumental in developing governmental and industry awareness of these issues.

We've got representatives of our many corporate leaders -- IBM and Dell and Oracle and Visa and more -- and, importantly, we have representatives of the advocacy and policy communities -- people like Ari Schwartz of CDT -- whose organizations play a crucial role in representing the interests of the individual in these discussions on the use of personal information.

So, I challenge each of you today to question the limitations of technologies, as well as laud the opportunities, and to remain vigilant to what we're now calling -- and here I give Marc Rotenberg of EPIC some credit -- P4T, the need to integrate people, policy, practices, and procedures with technology towards our goal of respecting the sanctity of the individual.

I encourage you to think beyond the ordinary framework.

There has been much conventional wisdom about privacy and security that has been more convention that it has been wisdom.

Privacy and security are not an either/or proposition.

Those who seek to make this country secure need not be heedless of privacy, and those who seek to ensure privacy do not necessarily seek to make this country less secure.

Let us remember and let us heed Franklin's words that those who would give up essential liberty to purchase a little temporary safety deserve neither liberty nor safety. Let us strive to deserve both.

Thank you.

(Applause.)

PANEL 1: The Process of Protecting Consumer Information:
Creating a Business Plan Using a Hypothetical

MS. LEVIN: Thank you, Nuala, for your remarks. They're very inspiring.

I just have a couple of other announcements before we get on with our first panel.

First, in your folders are the bios of the people that you'll be hearing from today, so our introductions are going to be very brief.

There are also hand-outs for the slide presentations, at least most of them, so you'll be able to take them home and not have to worry about jotting down lots of notes during the panels themselves.

All of this will be posted on our website, ftc.gov/techworkshop, so that you'll be able to view the other slides that were not in your hand-outs today and actually see the slides from the previous workshop, as well.

You will also find information on the website about purchasing videotapes of the two sessions, and later this month, we will have the transcripts of the sessions posted.

So, we don't want all the valuable information being presented today to evaporate in cyberspace. We want it to be there for you in the future.

For those of you who'd like to add to the record of the workshop, information about providing written comments on the topics of either workshop session is on the website, and the final deadline to submit comments is June 20th.

There will be a brief five-minute question-and-answer period prior to the end of each panel, and if you'd like to address a question to the panel, we ask you to line up behind the microphone, which will be in the back of the center aisle.

So, we're ready to begin.

Panel one brings together some of the leading privacy and security experts in the country to give you a glimpse, an inside glimpse of how we go about creating a business plan to manage privacy and the role technology can play in that plan.

Let me first introduce my co-moderator, Joe Alhadeff, chief privacy officer for Oracle Corporation, and then to my left, Gary Clayton, chairman of Privacy Council, Incorporated; Stephen M. Paroby, global director of markets for technology and security risk services of Ernst & Young; Steven Adler, market manager of IBM Tivoli Security & Privacy Software; David Chaum, a security expert and consultant, cryptographer and inventor of electronic cash; Susan Grant, vice president for public policy at the National Consumers League; Richard Purcell, CEO of Corporate Privacy Group; and Larry Ponemon, chairman of the Ponemon Institute.

Before we launch into our hypothetical discussion, we're going to learn about what businesses are currently doing to manage privacy, and Larry Ponemon will open our panel with a presentation of his 2003 benchmark study on corporate privacy and data protection practices.

Thanks, Larry.

MR. PONEMON: Good morning.

What I'd like to do is to talk very, very briefly about a study that has just been completed. It's a benchmarking study of corporate privacy practices.

I think Toby is going to hold me to a real tight deadline, because if you know me, you know that I like to talk and always go over on speeches like this. So, I will just touch upon the major findings of this research, and at your leisure, if you want to contact me, if you want more information, we could have private one-to-one conversations.

I will not bore you with all of the statistical details, but it's a very interesting study. Of course, I'm biased.

Let me just start off with some general reactions. You know, one picture is worth 1,000 words, and one general reaction is worth 1,000 pictures, and these are some of the comments that were provided to me, and these were not recorded on the survey instrument.

Of course, I'll start off with the most positive. “This survey was amazingly useful. It helped me to see all the activities that we aren't doing now very well.” And that's my mother. She wrote that one. I'm being honest.

“Frankly, Dr. Ponemon, after completing the instrument, I was embarrassed to submit because of all the ‘no’ and ‘unsure’ responses.” That was an honest response.

Number three. “I make no guarantees about the quality of the enclosed responses. It was completed by my boss, and he is likely to have been wearing a pretty big halo when editing my work.”

Okay.

And “Larry, I like the survey very much, but I don't really think all this research will make a difference. The only measure that is respected around here is return on investment. Is there an ROI for privacy? If so, tell me about it soon, because I'm drowning.”

These are real comments.

Four basic questions.

When you do research, before you start the project and you're trying to be objective about your work, you are really asking these basic essential questions:

What are you trying to accomplish? And in particular, what are leading companies doing today to ensure adequate compliance?

Is there a common set of business practices employed by leading companies to ensure reasonable protection and controls over personal information?

Are there apparent gaps in privacy and data protection activities that may create some vulnerabilities for companies?

And then last, and certainly not least from the

FTC's perspective, do corporate privacy and data protection practices vary across industry sectors, and if so, perhaps there's an influence of regulation, or the lack thereof.

Now, again, I promised some caveats. Before we get into the findings, the focus is on description. This is not normative research. We're not testing specific hypotheses. It is based on a small, non-random, representative sample of companies.

So, to the extent that companies participated, you can assume that these are probably companies with more mature privacy programs.

There is an enrollment bias. We believe that larger companies will probably have a better privacy and data program than smaller or younger companies, and unmeasured organizational factors -- and they are many and too numerous to mention right now -- that may explain differences across companies.

The halo issue is always an issue in research of this kind. So, there is the possibility that this self-reported data is just overly positive, and doesn't reflect reality.

Now, a little bit about the instrument.

Many of you have seen the instrument, and again, if you're interested in seeing all of this gruesome detail, I will make it available to you. It's in the public domain, and this was work done in collaboration with the International Association of Privacy Professionals, the IAPP. So, the benchmark survey was developed and refined with a learned group of experts, 11 corporations and one Federal agency, and these are CPOs or senior executives representing privacy.

The instrument was organized into eight core areas representing, actually, 108 different topics. So, there are 108 topics organized into eight areas. You might actually think about it generally as issues that chief privacy officers face or the business processes that they're trying to manage, such as policy, communication and training, privacy management, even data security, compliance and monitoring, choice and consent, global standards, and probably last and certainly not least, redress and enforcement.

Methods were survey driven, but in many cases, we decided to do diagnostic interviews to learn more. Sometimes the responses were sorely incomplete and the only way to get to the meaty data was to talk to people, but we did promise confidentiality. So, unless someone revealed the name of the organization, we could not have that one-to-one dialogue, but in many cases we did.

The final survey was distributed at the IAPP annual summit in February. We received 111 total completed surveys, of which we rejected four because there were internal inconsistencies. You hate throwing away research as valuable as this, but we just felt it was low reliability. We got rid of them.

So, we had 107, and of the 107, one of the questions we asked, are you a small company, that is with a head count of less than 5,000, or a large company, and that one variable explained probably 60 percent of the variation in privacy practices.

So, we decided for this research to do two studies. We're going to do a small company study and a larger company study, and we are now reporting today on the larger company results.

An illustration of the survey instrument itself -- we try to limit responses to "yes/no." If you couldn't respond "yes," or you couldn't respond "no," you had "unsure." If you couldn’t respond "unsure," you could leave it blank, and there were places for noting exceptions. So, there were many exceptions.

The primary dependent variable of analysis is something that we refer to as a percent positive response. It's the percentage of "yes" responses, "yes" denoting something that is good, "no" denoting something that may not be that good, and there were reverse-scored items, so "yes" is really a positive response. It's not always the "yes" response to the survey.

Industry classification. Because we're dealing with 55 larger companies, many of which are Fortune 500 or Global 1000 companies, we did not cover the waterfront of industry.

The largest industry concentration is financial services.

We grouped health and pharmaceuticals together, and for those people who are in the pharmaceuticals industry, please do not throw anything at me, because I understand that that's not true. Pharmaceuticals is manufacturing, but it also covers some major health care issues, so they are grouped together.

We have consumer products, manufacturing, retail, telecom, the automobile industry and a transportation company, technology, and other. Other includes one Federal agency.

Now, the results.

Based on that percentage of "yes" response, companies are doing probably more around the privacy policy than any of the other categories.

That's a good fact.

The bad fact is redress and enforcement is not being attended to very well.

Data security, privacy management, communications, and training -- the compliance-oriented activities -- are taking the lead.

Issues like preference management, where there's 41 percent of compliance, or of percentage "yes" response. Attending to global standards, because all of these companies, save one Federal agency, deal with the international regulatory issue, not just the Federal or state regulatory issues, and global standards is not a high priority right now.

Now, industries vary, and this is interesting, and this might suggest, if you are pro-regulation, that regulations make a difference, and you will see that financial services do better in terms of the percentage "yes" than other industries.

Well, don't get too excited, because health care and pharmaceuticals, which some would argue is subject to even more regulation, is at a very low level of compliance.

Unfortunately, one cannot conclude that regulations are playing a big part, and the fact that you have a 64-percent compliance rate may not suggest that companies are doing very well even in financial services.

Also, the automotive industry, for some unknown reason, seems to be stepping up to the plate in terms of basic blocking and tackling.

So, of any industry group that seems to be pro-actively managing this thing, it's probably automotive, but keep in mind, the big automotive companies also are financial service companies.

Now, I'm going to rush, because I feel the pressure to get to the panel.

Key findings -- I'm not going to go through all of these, but on the positive and negative side -- and these are just examples. I say key findings, but these are example findings. There are many, many more in each of these categories.

Almost all of the companies have a privacy policy, and the majority of companies get approval at the CEO and senior management level, and there are formal controls over revisions to that policy. There does seem to be an alignment between the policy for privacy and the ethical conduct policy, which we think is a good thing.

There's also a separate policy for employees.

On the negative side, the policy doesn't seem to be aligned with major stakeholders. No one ever talks to the consumer or the customer or the policy holder or the person that you're trying to protect. There seems to be a real gap. We think we know what they want, but there's no evidence to suggest companies do research in this area. They do a lot of marketing research but no research on this issue of what consumers want.

Policies are still way too complicated. If you use the eighth-grade reading level, this is at the 29th-grade reading level in some cases. But it's very, very complicated, and people just don't understand it.

There's also very limited disclosure. Unless you're require to have a notice, most of the disclosure might be web-based disclosure.

On communications and training -- well, good news -- there’s widespread communication of privacy policies to employees, nice outreach. That's good. Policies are shared with business partners. Good deal. There’s widespread communication of policies to customers and even consumers. Good thing.

On the negative side, very, very few organizations open up their compliance program to key business partners.

There is no privacy awareness activity in most cases to customers, no mandatory -- underscore this word -- mandatory -- or very limited mandatory privacy training for employees.

No computer -- very limited computer-based training activity -- and you would think that's the greatest way of educating people, a low-cost way of doing it.

Do not report training results to senior executives of the board, which is a surrogate for accountability. Don't even measure effectiveness -- you're going to spend millions of dollars. You want to know if there is an ROI, and a lot of companies aren't really measuring effectiveness at this point.

Key findings on privacy management: Probably the most positive of positives is that the management of privacy is not that department off to the corner and no one knows what they do. Rather it's a cross-functional team, and that is the right way to manage privacy, in my opinion. That's good.

Privacy committees have formal responsibilities and a charter. Very good.

Business partners must comply. At least, people tell us that in the survey. This may be a halo effect, but they must comply with the privacy policy.

Well, the number one negative in this category is 52 percent believe there is a serious, serious lack of resources to achieve privacy goals. If there is one issue that was communicated to me off the record, that was the off-the-record comment that we can't get our job done without a budget, and we just don't have any.

Privacy is not important to executives for brand or marketplace image. This is the perception of the CPO. Yet when I talk to marketing executives, they do believe that privacy is important and it's a way of engendering trust. There's a workshop on the 18th that's going to get at the value proposition to privacy, and I think this is one of the issues that we need to discuss.

There doesn't seem to be a direct reporting relationship to the CEO or senior leadership. Although CEO's are involved, it's not a direct involvement.

Remember I said we will hold our business partners to our privacy policy? Good fact. How do you do it if you don't monitor, okay? Forty-five percent of the companies are not monitoring it. At least they tell us -- this is with the halo -- that they're not monitoring those policies. And very few organizations actually conduct independent privacy audits, which we think are good. I'm somewhat biased, having been a privacy auditor.

Key findings on data security -- and I'm going to go through these very quickly, Toby.

Positives:

On the positive side, companies are actually trying to take stock and inventories of their personal data.

Here's an interesting fact. There is an

evaluation of new software applications. As they are entered into production, companies are at least looking at some of the privacy and data protection issues.

And perimeter controls -- data security, at least over consumer-centric data, seems to be pretty good, and employee data, as well.

The issue of honoring consumer preferences -- 66 percent don't have a mechanism for doing that, and actually, Steve, you'll talk about IBM, but tools like that could actually make a big difference.

No integration of information security with privacy initiatives.

You would think that these are hand-in-glove concepts, but many companies still operate these two in silos.

Lack of control over IT. For example, basic issues -- who controls website domains?

I can't tell you how many companies said, I know there are websites out there with our company name on it, and I don't know about them, and I know it's going to get us into trouble.

Widespread use of our favorite thing, the Social Security number, still exists as a primary form of identification and maybe even authentication.

Low use of privacy-enabling technologies. What was interesting about that is companies are really interested, but they don't have the resources right now. So, CEO's need to step up to the plate or we have to do a better job of explaining the ROI, so people see the value.

And a low usage of P3P.

Key findings on compliance:

Senior management support privacy compliance programs. At least they say they do have them.

Privacy compliance is viewed as a significant regulatory concern for the company, and privacy and data protection strategies are actually in place today, but there's no crisis plan, in many cases.

Companies wouldn't know what to do if they were hit on the side of the head with a two-by-four. Unfortunately, that's reality.

They don't check things like marketing campaigns to determine whether those campaigns they're marketing are privacy-compliant.

They don't use internal auditing that's available to them to monitor privacy.

And they don't conduct mock regulatory assessment or audits to see, if the regulator showed up on Monday, that by Friday, when they got the opinion, it wasn't a negative audit opinion.

Very briefly, choice -- you notice the list of positives keeps getting smaller and smaller, and negatives actually get larger. The issue here is that opt-in is not used, and I know it depends on the industry sector, but it's just not used. There’s no flexibility in how consumers and customers communicate choice, and this is interesting, because consumers want better ways of telling the company how they want their data used and how they want to be respected, and companies aren't doing it or doing it well. Employees are not given a choice over how their PII is collected and used. That's the sleeping tiger or giant, the employee issue.

On the global side, we all know that evaluation of global standards is done, but compliance with these laws isn’t monitored.

Transport of data flow issues, new Canadian regulations, and even the issue of safe harbor -- it's just being ignored or it's not considered as a high priority in many cases.

The redress area has probably the greatest gap.

For the most part, organizations just don't have it together here. They don't have a clue.

Many companies actually are doing it well, so I don't want to just generalize to every organization, but the vast majority of companies are just not doing a whole lot in this area.

Employees, for example, don't have a process to resolve concerns about their personal data. Consumers and customers can't access and correct their personal data. There is no redress program for consumers and customers. There is no process for enforcing privacy violations, and that's a depressing fact.

They do not have a process for reporting privacy complaints to management, and that is interesting because state laws, such as in California, as you know, now have time-lines.

An issue occurs and you have a time-line for getting something done, but many companies are not aware of that, and they're not imposing any reporting time-line.

It goes into a great void when a complaint is registered.

So, what did we learn?

In summary, many companies are actually achieving modest success, even with all the negatives, with their privacy and data protection program. One of the questions that we asked is do you feel that the world is getting better for you, and the good news is that most companies, even with these negative, dismal findings, are saying yes, they expect to spend more money, and they really viewed the technology area as the area of greatest hope. So, it's enabling technologies that, at the end of the day, will make the difference, we think.

Companies are vulnerable to privacy breaches because of gaps.

The gaps that we've identified -- just having a policy doesn't mean you're doing much. You have to do more than that.

And companies are moving in that direction, but there are still some pretty large mine-fields to be aware of.

Certain industries seem to perform at a higher level of compliance -- for example, the financial services industry -- but I don't think we can draw the conclusion about regulation, as I mentioned before. So, it is still unclear that regulations for privacy and data protection serve to improve or hamper the leading practices or best practices.

I'm going to close, but I think the key variable is there's a lot of data here, and we're very proud of our report. For anyone in this room or anyone you know, if you're interested, just give me a call, and we will send the report to you.

Thank you very much, and now I'm going to turn it over to Toby and Joe.

Thank you.

MS. LEVIN: Thank you, Larry.

(Applause.)

MS. LEVIN: As an agency that's very interested in studies and surveys and empirical information, we appreciate your having done the study, and we look forward to analyzing it in more detail and talking with you about it.

There's an executive summary of it in your folders, as well.

Now, I'm happy to turn it over to Joe Alhadeff, who is the author of this very challenging hypothetical. The description of the hypothetical is in your packets, as well, and he'll walk us through it.

MR. ALHADEFF: Actually, I had asked Toby to get a Lavaliere so I could do an Arthur Miller-style discussion with this hypothetical, but I don't think I want to. I won't challenge the person who is trying to do the video by having me as a ping-pong ball walking around the room. So, I'll just moderate from my seat, if that's okay. That would actually give you another option for Commissioner Swindle's comment that everybody move to the center if you actually want to see us.

We have essentially a two-part hypothetical. It's one fact pattern, but it's going to be dealt with in two parts.

Part one is going to be the brainstorming session of the consulting group, whereas part two is the consulting group doing the presentation to the client. By way of background, so that you don't have to read through the entire hypothetical, there's a consulting group called Consulting and Advising on Net Deployment and Operation -- a catchy name, CANDO.

The firm specializes in technology and policy consulting on Internet and deployment, and the firm that they hope to work with is a firm of retirement communities called Golden Oldies. They're a confederation of retirement communities that essentially have six locations -- five in the U.S., one in Canada.

The communities have doctors on-call. They provide small clinic facilities, pharmacies, libraries, some convenience services, including in-home meals, shopping, and some financial advisors.

So, the CEO has had a meeting informally with one of the representatives of CANDO, and the CEO is, oddly enough, a gentleman named Ivan Offerforyou, and he went to a trade show -- it will sink in over time. He went to a trade show, and his concept is he wants to have wired communities, because he's seen that this is the next big thing. So, they've gotten some computers in the community centers and the residents seem to be liking it. They've gotten broadband out to the home, but a lot of the people in the community don't have computers yet, and he's starting to think big.

He wants to try to group the purchase of the computers. He wants to try to start grouping the purchasing habits of some of his residents to get them better price advantages. And then he's also thinking from an administrative point of view about his six offices that have essentially been working in non-modern times in terms of technology.

While they each have a computer, the computers aren't connected, and they've been exchanging data by sending disks back and forth or even sending print-outs back and forth between headquarters and the various community facilities.

So, he's trying to figure out how to work this forward. One of the other things that he's looking at is all of these community centers purchase products, whether it's to stock the small grocery that may be in the community, the cleaning supplies, the medical supplies that the little clinics may use, and he's figuring that group purchasing there might be beneficial to him, also.

Unfortunately, as part of the description that he has given you, one of the concepts that he wanted was to have you guys come in to give him advice on what package he needs to buy to solve this problem.

The other thing that he's figured out is that, while it's a big operation, it's a family-run operation.

So, as CANDO, you may be starting to wonder about the professionalism of some of his staff.

Many brother-in-laws and cousins who otherwise were unemployable seem to have found a job somewhere in his organization.

Technologically, they have some tech people on staff, but really, they're kind of Mr. Fix-It's. They show you how to use a piece of software but they don't really interact with the residents. They only support the people within the community who are administrative staff, and they work on that one server.

I will make one comment about the process here before we get into the flow, and the process is, if you look at what you've got on this panel, in many ways it could be a dream team of consulting. I mean CANDO could be CAN'T AFFORD.

And so, I don't want people to presume that you need a team of this variety and experience, necessarily, to have a solution.

We're fortunate in the fact that we've been able to attract this team, but there are lots of people out there and lots of ways that you can get this advice at a much more affordable fashion than what you've got sitting in front of you.

This is a great opportunity, and Toby and the FTC have shown amazing courage in letting the egos that are sitting on this panel, who could each fill up the hour-and-a-half time slot by themselves, interact without a net.

So, with that, we'll plunge into the deep end and see where we go.

MS. LEVIN: For the first part, all of the panelists are part of CANDO, and we've got our logo sign right in front.

During the first part of this hypothetical, everyone is part of the discussion.

MR. ALHADEFF: None of the information that the panelists now have can be imputed to them when they become an officer of the company in part two.

Essentially, this is the brainstorming meeting.

We're now called to order. Just looking at this, we're trying to figure out what it is that needs to be done for GO -- Golden Oldies is going to be abbreviated as GO from now on -- for GO to develop a business plan. The first question, which I'll ask my colleague, Richard, is do we have all the information we need? Is there something that we don't have here? Do we have the facts?

MR. PURCELL: Well, I think we have the framework. I don't think we have the facts.

I don't know what the age span of the people here are.

I don't know what their particular interests are.

I don't know how far away from their relatives or other communities they live.

So, there's a whole bunch of connectedness that I need to know.

The other thing is I haven't seen yet what the platform is they're running on or if there's any consistency across these six different operations in terms of the platform. How are they transferring this information?

Steve, have you heard anything about that?

MR. ADLER: I'm sure it's a LINUX platform.

MR. PURCELL: Oh, you think so. Well, it probably is, because they're the brother-in-law kind of thing, right? So, they're going on the cheap. They definitely are patching this thing together.

I'm wondering if they are putting together a consistent data exchange here at all. We know they're shoving diskettes at each other, so obviously they're not very consistent.

MR. ALHADEFF: I think we can't presume that there is any consistency within the data. As far as your issue of the ages of the residents, he had said there was seemingly some variety, but we know that the family members want to interact.

Steve, do you have any thoughts on things that we would have to look at in terms of some of the issues that we would first see?

Richard's pointed out some of the information we need, but are there big gaps in the information we have. He's looking for a turn-key solution, a package, and I think maybe we need some foundation.

MR. PAROBY: Well, I think in any organization, no matter what size, no matter what they're into, you first want to start with their vision, their strategy, their mission, their growth plans.

Currently, where are they? What's their current state?

And you mentioned what's the platform? What are they running on?

What are they doing? What's their connectivity? And you have six centers, but how many people? What age groups, et cetera?

But I think the strategy, the overall vision, the growth plans are something that you would start with in any organization before you make a determination on what to do to solve a problem.

MR. ALHADEFF: Susan?

MS. GRANT: I think there's a big missing piece here that I've noticed, and that is that we don't really know what the residents of these communities want.

We haven't had an opportunity to survey them or talk to them at all.

I'm not really sure, talking to the people in the company that we've interacted with so far, that they know what the residents want.

I think that's really important.

MR. ALHADEFF: Larry, is there something that we can at least gather from him as to how we'd phrase the goals that they seem to want to accomplish?

MR. PONEMON: Yes. I think it goes back to value proposition, and even though I think we understand what it is, we need to have the client tell us what that value is, and then we have to see whether, realistically, we can meet that value.

MR. PURCELL: Well, yes, value, but what about affordability, too? I mean it's a pretty small shop.

MR. PONEMON: The key is it's a value-cost argument. There could be an unlimited amount of value, but it's just too costly because it's a small company. So, that also has to get into our equation somewhere.

MR. PURCELL: So, don't we have to figure out what we can do for them and what we can't, as well?

MR. ALHADEFF: I think one of the things in terms of what we can and what we can't do is -- we haven't really established what role this community center wants to play for its residents, which is something that Susan has highlighted, and a couple of other people. David, it struck me that they're talking about a lot of things which will involve purchases, but there hasn't been much discussion about how you're going to buy anything or what you're going to do.

Do you have any thoughts on some of the issues that might come up there?

MR. CHAUM: In view of keeping the cost low, they could just take advantage of some of the currently available anonymous payment systems and ordering systems so when the residents are obtaining pharmaceuticals and groceries and all that sort of thing, checking out books, they could do that anonymously and without having to invest in systems themselves.

MR. ADLER: The only thing I would add is that we don't know yet what their application infrastructure is, what their network topology is, what they're using their applications for, what their business processes are, what their data flows look like.

There are a lot of questions that we need to figure out -- if there are six different resident communities, what does that infrastructure look like? How primitive is this? And what types of personal information are being collected, and what's being done with that personal information? Are there any controls internally at all?

MR. ALHADEFF: From a gap analysis point of view, I think we've identified a lot of the technology gap analysis.

Gary, could you highlight some of the policy gap analysis that may be there or some of the issues that they haven't been thinking of that are perhaps non-technological?

MR. CLAYTON: Sure. I think starting from the idea of a data flow, clearly there are a couple of things that come to mind here.

As to the HIPAA requirements for protecting some of the information that may related to health, it's not clear what they're getting or how much of it would be covered by that law or what's being shared among the entities or even what's needed to be shared among the various entities or the outside deals.

They want to offer financial services, and that raises a question immediately of Gramm-Leach-Bliley and the protection and security provided for that information.

Also, what are they thinking with respect to providing either the health or the financial services? Are they really going to offer it internally, or is this going to be someone who's just simply going to be using access to their facilities to offer it?

It goes back to the data flows. What are they getting from individuals? What do they hope to get? How does it help their business?

What I would hope we point out to them is, one, you may not be able to afford a Mercedes today, but you certainly can start things, and you can start implementing. Then, secondly, you've got to understand and manage this process. They may not have any of the resources internally to manage it from a privacy or security perspective, particularly since they're all brother-in-laws and the like that are involved.

MR. ALHADEFF: So, you're suggesting maybe they get a Chrysler, which is a Mercedes by another name.

MR. CLAYTON: Something like that.

MR. PURCELL: But Gary, isn't it true, also, that we have to be careful, because whatever we do for them, whatever we can implement, won't they also use that for unintended or unanticipated uses?

You set up a whole network for them to communicate and to get this data exchange going. Won't new data be introduced into that process, as well?

MR. CLAYTON: Absolutely. And one of the messages we have to give is none of this is solved by the silver bullet of technology.

There are going to be people, processes, procedures in place, which goes back to what do they need, how do they need it?

And I think one of the things that we need to stress to them is managing their information systems is going to be integral to their business process -- it’s their supply chain, their business. This is not just an external part or a little piece that's added on the end.

It's got to be an integral part of management to keep exactly what you're talking about either in control or to make sure that you take advantage of it where you have opportunities to do so.

MR. PURCELL: So, you're thinking of putting in a training or a staff development component to what we're talking to them about?

MR. CLAYTON: We need to ask what training they have, what awareness they have. One of the things that strikes me, particularly with a group of older Americans who may be using technology for the first time, are issues of identity theft and fraud.

So, the training is not just for the employees or the service providers. It's also for the residents of the communities.

I think there are huge issues, particularly if they really want to fulfill their goal. They've got to feel comfortable.

And I think the final thing would be one bad act by someone as an employee or a couple of bad incidents against a couple of the residents would probably kill any programs they have.

So, it's very important for them to understand the possible consequences. That's their return on investment. They've got to handle all these issues, in some ways, if they want this program to work.

MR. ALHADEFF: Part of what we've heard -- and perhaps the suggestion that he's looking for, especially when he talks about wanting to lower the price of things for his consumers and wants to benefit the residents in different ways by the services -- is he seems to want to create some value in his brand and maybe differentiate that. Do you think that we can use technology and some policy advice to help him to do that?

Larry?

MR. PONEMON: Well, it goes back to what is the goal?

Is the goal to get the elderly folks in the nursing homes to communicate, and this then becomes a reason for choosing this organization versus another organization, choosing one retirement facility versus another. Maybe it can be baked into the trust proposition that when you do this, when you make this choice, your data is protected, plus you have access to the best and latest technology, and this is a good fact.

Just one point. I just want to echo what Gary and Richard said.

The issue is not just about technology. It's about people. And people want to use information in ways that are just wonderful -- for example, talking to your physician and/or talking to your grandchildren by e-mail and sharing confidential information -- but there are risks associated with that.

So, somehow, in order for the trust issue to work, you have to overcome those risks.

MR. PURCELL: Are we better off by out-sourcing this, by making a recommendation that it just be handled out of house totally?

I don't know where we are in terms of our decision to recommend to them an internal decision versus some packaged service provision that they don't handle, that they just hire out and it's totally out-sourced, but it's a reasonable thing we should talk about, right?

MR. ADLER: It doesn't address what Gary talked about, this human dimension, or that Larry was also talking about, in a sense, transforming that infrastructure. We need to put in place a human dimension where people who may not have the level of technology comfort that we enjoy can nevertheless feel they're being taken care of in the way they're used to be communicated to. There is a requirement here that out-sourcing won't address, and that's the transposition of whatever management and technology infrastructure we put into this dimension of people's needs and how this integrates into their lives to add value.

That's really a critical component that out-sourcing won't address.

MR. PAROBY: They seem to be looking for the silver bullet, as you mentioned, when, in fact, they may not need the silver bullet.

They need the bricks and mortar of a foundation or a framework, as you said, Steve, before they get to that. Technology could be an enabler. Security and privacy are enablers. They could be a brand differentiator for them as they go forward, but I think they need the foundation first.

MR. ALHADEFF: Richard raised the out-sourcing point. Susan's also raised the importance of bringing together some of the human factors and making sure that the human factors are addressed, which is what Steve was talking about and where some of the out-sourcing benefit would stop. But I think what we're looking at is out-sourcing the way that you manage and handle the back end.

As we've figured out, the tech people that they have on staff seem to be fairly limited, but what Steve's talking about is then how do you get to the residents what they need, which is really the front end, and that's, in many ways, the differentiator.

We haven't grappled with one concept, which is he's also wiring the communities for administrative purposes, and he's going to take a look at those communities and try to figure out how they can do purchasing and how they can do information communication.

Do you see any issues that come up on the administrative side, when they're wiring and communicating with each other, versus on the residents side?

MR. ADLER: You mean in terms of management oversight over the communication infrastructure?

MR. ALHADEFF: And also how the communications structure works on the theory that one of the communities may not be in the United States. I was just wondering if that raises any flags for anybody.

Gary?

MR. CLAYTON: Yes. Clearly, we need to make them aware that Canada has a different privacy regime than we do in the United States and so different laws, different issues arise. It may impact the ability to even get some of their information from Canada to the United States.

I think we need to understand what they want. Going back to the issue of expense that Richard just brought up and the idea of whether you manage or not, I still don't have a real good sense of how much of an urgency this is for them or how much money they want to spend, what's their budget, and what's really their business goals other than these broad, general aspects.

And I think before we can answer the issues about Canada, we've also got to look at the issue of which states that they're in -- whether you're in California with some specific requirements there or you're in other states that have limitations -- you may have a whole host of issues. Ironically, one of the things that strikes for me for a group like this is there's probably going to be a lot of grandchildren coming in and using the technology. This presents issues that we would never think about for an elderly community, including some of the child protections that the FTC administers.

MR. PURCELL: Well, you know, their presence in Canada cuts both ways, too.

Let's remember, they do buy a lot of medical and pharmaceuticals, and getting those from Canada, through that facility there, and then trans-shipping them to the States may be really advantageous to their cost, too. So, let's make sure that we're thinking about how we can make a pitch here that works for Golden Oldies, not only for managing their information but also managing their operational infrastructure, too.

MR. CLAYTON: Yes. I really think that there are two things here that are important to them that are our big sales features. One is providing efficiencies within their management so that they can run at a more cost-effective basis. Another is providing much better services and serving the needs of the people who are living in this community.

These are retirement communities where people actually opt to live and they pay relatively big bucks to live there.

Nonetheless, I think that considering the fact that GO may not be able to do everything that they want to do at once, once they figure out exactly what it is that they want to do, maybe what we can do is present a plan that is incremental, so it can be phased in over time.

One other comment.

One of the things I think we need to stress is so many people view privacy and security as just a cost, an add-on that's something that's a burden on them.

There may be well ways that not only can they improve their brand, but they can actually make money by doing some of the things well, even on the privacy protections and some of the security protections, that's more than just, we have it and other people don't. If we understand their business and what they're trying to do and keep looking for those answers, it may be one of these arguments where they literally pay for some of these things through their own improvements that they make.

MR. CHAUM: Part of the scenario, I believe, is that the residents themselves will get managed computing power from GO, and that opens up the whole opportunity to provide all kinds of consumer protections on those machines, from anonymous surfing to child protection and so forth.

So, I think their computing systems could be a profit center.

MR. ADLER: There's a modernization, electrification, automation process that's going on here for a family-owned business that heretofore hasn't had tremendous communication integration. We have to provide not only that new communication infrastructure but then both the technology and the process and the transparency above the integrated management structure so that these new collection features don't introduce risks and uncertainties, or make customers or residents uneasy with this migration to a new platform. It’s a new way of communicating with their organization.

MS. LEVIN: For a lot of people, privacy has been thought of as a privacy policy, and what I hear from all of you is that privacy really is a business management process, and in fact, you get a whole lot more out of it than just a privacy policy. Is that right?

MR. ADLER: It's an operational challenge.

MR. ALHADEFF: I think one of the things we have to be careful of here is something we heard about in the report we got on GO’s first request.

Ivan figures that if he takes the paper out of the process he's done. Taking the paper out of the process, even if you're just looking at optimization, is about 10 percent of the battle.

We have to figure out how we can optimize some of his processes for this new environment that he's working on. We've all spoken about the need for a value proposition. I figure that we're going to hear from him -- what's my return on investment here?

MR. PURCELL: Yes, I agree. A lot of what we're talking about is the data security, data privacy, the control of information.

I'm not so sure that's what Ivan is that interested in.

He wants operational efficiencies. He wants to stop bleeding all of this postage and writing disks and so on. They're in a very insecure operation right now. I'm not so sure he's very tolerant of that. So, we've got to pitch a little bit about what the exposure he's currently under is all about, how he can resolve that and still get operational efficiencies.

MR. PAROBY: We don't just talk dollars for operational efficiency and a return on investment.

I agree that that's probably what they're going to look for, and I think we need to talk about both the tangible and the intangible benefits or deliverables that could come about from a safe, secure, efficient environment.

MR. CLAYTON: And I think one other point to make is he may already have a lot of these obligations and burdens and risks in place already, as you talk about them. Just because he's in paper, it doesn't mean that HIPAA's not going to have implications for how you at least manage some of the information, particularly if you end up mailing it, by disk, or transferring it out.

So, I think he needs to understand that just by putting technology in place, it's not going to cause all these solutions to have to come to bear.

MR. PURCELL: He obviously doesn't understand this just today. We're in character development now, but the way they're operating today, they're not getting a lot more requirements if they make any kind of transition than they're under already, transition or no.

MR. ADLER: So, what I think I'm hearing you say is that we have to make this part of the solution --

MR. PURCELL: Yes, I think so.

MR. ADLER: -- not an obstacle to data sharing or communication, not an additional cost burden outside the system, but that data handling practices, privacy management, training, infrastructure have to be part of the way the solution is presented.

MR. PURCELL: I agree, yeah. I think these are challenges that GO already has in the off-line world that they're not addressing just because it's not the way they've done business before.

As they transition into the digital world, it's not a new obligation. It's just that the obligation becomes a little more apparent.

MS. GRANT: We need to help them assess what they're doing now, see whether they need to change any of that, before they transfer all of this to the automated world.

MR. PAROBY: And that's an issue -- you just hit upon it. Take any organization worldwide. They try to find the silver bullet -- they try to find the quick fix. They try to get a software package or a consultant to do something to take them to the next generation.

However, 99.9 percent of them don't know their current state, don't know the risks they have, don't know the environment that they're operating in, don't know the rules, don't know the regulations, and in many cases, they're afraid to take that step to find out where they are and find out what they're doing right or wrong.

MS. LEVIN: Larry, you've been waiting.

MR. PONEMON: This is like my dinnertime conversation with my family. I have to really fight to get that word in.

Two things.

Number one, we're supposed to be a group of consultants, and it's interesting. We do consulting because we think we know all of the answers. Susan mentioned something that was critical to this whole process -- alignment, understand the value, talk to people. I'm thinking of my mother, who is now 82 years old. She's going to kill me for saying that, but she is 82, and she lives in a retirement community in Arizona. She calls herself the little old lady from Tucson, and she has a website -- I'm serious -- called littleoldladyfromtucson.org. This lady is like an Internet nut.

For her, the number one issue is convenience, convenience. She loves it. The number two issue is cost savings. She loves it.

Number 19 on her list is privacy and data protection, because she'll say, look, I'm 82, I'm going to die, my data is useless, I don't care, exploit it.

But to some folks, data protection is the sleeping giant, right? It's what, Gary, you were talking about, that you may not even see the risk. So, what you have to do, as part of this team, after we align and understand what the real issues are, then we need to educate businesses, because they may be completely insensitive to the data protection risk.

MR. ALHADEFF: I'm going to get a little structural.

MR. CLAYTON: May I just make one point?

One of the things I think we also need to at least approach with GO in this meeting is you don't have to do it all at once.

There are things you can do now. I don't know what we would start with, but it seems to me that part of the initial effort is what the heck do you want first and how do we help you get there. Going to Larry's comment about what do people need, they may have six communities of Larry's moms that are all technically savvy, using the Internet, and that would dictate one path. They may have someone like my father who has never seen a computer. We just need to understand the situation, and they need to be able to give us some roll-in, if you will.

MR. ALHADEFF: Larry's mom can do the training sessions.

We've got a short amount of time before we're going to have to start meeting with GO, so I want to get to the issue of how we're going to structure our concepts. We've been a little bit all over the map, and we've heard that there have to be concepts of how to bring out the benefits. We have to somehow educate them about the risks and then somehow provide them the concept of a path forward.

Do we think there's a better approach in terms of how we present this? Do you start with the stick and move to the carrot? Do you start with the carrot and move to the stick? Do you not talk about one in the first meeting and the other at another meeting? What do you think?

MR. CLAYTON: In one sense, you've got a willing audience here that a man clearly is excited about a possibility, and I hate to put a damper on that by starting off with -- you're doing bad things, you're going to have risk, et cetera.

My sense would be we ought to play to the positives -- the cost savings, the benefits, the increased community, return on investment, and as part of that, a cost analysis, just what's it going to cost, what are the risks?

I would hate to start with the cost and the risk before we get to understanding what the benefits are.

MR. CHAUM: Unfortunately, I'm not going to be able to be representing the firm there, but I think one of the big selling points might be a real nice service that we could offer to the actual residents to protect them in this managed manner, and I hope someone from our team will --

MR. PURCELL: Yes. Can we split that out? I mean there are some categories of operational efficiencies here. One is their administration. What about their billing system? What about their provision of services for their medications, for their convenience items, for their community time schedules, all of that kind of thing? Then there are their operational communications within the network of the community.

So, you've got the internal community network. Then you've got the inter-network between these different six communities, including the Canadian facility, for operational efficiencies.

That includes supply chain management and all that kind of thing.

Then you've got the residents interacting with each other in that inter-community and the residents interacting outside of that community.

So, I guess there's four different interactions going on there, you know, the administration internal, the administration inter-network, the community internal, and the community inter-network.

MR. ALHADEFF: That's one thing we haven't discussed. Ivan’s never brought up the requirements that we've identified as things that he might need to do because of external legislation and things of that nature.

So, I think we're going to have to figure out how to address that, but Richard's raised a very important point, which is point three.

He's never talked about whether the communities could talk to each other and whether, within a community and across communities, there's any benefit he can bring.

Do you think that's something we should be emphasizing to him?

MS. GRANT: If they don't bring that up, I think we should.

MR. ALHADEFF: You know, those are the kind of things you were talking about earlier, David, about having anonymous communications.

I would assume when you're talking about personal communications inside the community, though, you're getting to less anonymous, or are you.

MR. CHAUM: I think the residents could correspond with each other under first names or something like that, in a way that was partly anonymized to the outside world. I think we can have suggestion boxes, for example, as a way for residents to communicate anonymously with the organization itself that might be very helpful.

MR. PURCELL: How else are Gary's dad and Larry's mom going to get together? A lot of these communities want community. We've got to be careful, because to a certain degree we've heard in some of these conferences we've been to that privacy is a middle-aged problem. A lot of our parents' generation and our younger generation care less about these kinds of issues than perhaps we do. So, we have to be very careful to make sure we understand what this community really does want, whether it's anonymous communication or not.

MS. GRANT: And you know, it may not be one community either. It may be that there are differences in the different parts of the country in the U.S. where these are located, as well as in Canada -- differences between the residents in terms of how they view privacy, and I think that's important to get at, as well.

MR. ALHADEFF: I think we've got some issues that were being fomented on this end of the table.

MR. CLAYTON: One of the other things that I think we need to just talk about -- and we talk about these people as though they're fungible residents -- is accessibility and issues related to that.

You may have people, in this community,

particularly, with poor vision, poor hearing, an inability to really access some of what’s available through the Internet. We've got to be able to at least understand what those issues are. Secondly, as you said, Richard, he hasn't given us any information so far about whether the communities are communicating among themselves, what the telecommunications systems are, what sorts of lines they have. I know that they have cable modems they're trying to put out, but those raise issues by themselves.

So, I think we need to get a little better sense of really how do they hope to communicate if they're trying to form one community?

MR. PURCELL: Yes. Accessibility is a good point, Gary, because when we pitch this company, they've already got to be living with regulatory overheads, right?

By telling them that there are additional regulatory overheads they may not be aware of, it's not new to them. They have accessibility and ADA regulation that they must be under and be used to.

MR. ALHADEFF: They have someone already who does compliance, but his compliance has not, so far, been HIPAA or Gramm-Leach-Bliley.

His compliance has been because they have some pharmaceuticals and things of that nature. It's more on the insurance side of life where they've been filing, because they actually haven't been operating the pharmaceutical entity within the group.

But it strikes me that we raise an important point about the residents’ expectations. In some ways, are we projecting some protections onto them that they might not want?

Susan started out saying we need to survey them. David has pointed out that we need to offer them the choice of how they want to communicate. I think we have to be very careful not to indicate to them that we know of a solution that's good for them which they may not decide is good for them.

So, do we have a technological and policy architecture that's going to be flexible enough to offer them a broad range of solutions, or does that just become cost prohibitive?

MR. ADLER: So, you're saying that we want to offer them a foundation or a tool kit that they can use themselves to determine how they would like their information used.

MR. PURCELL: Well, I'd be careful with that.

MR. ADLER: Instead of imposing a regime or even trying to pre-survey people and base a regime on survey answers, where consent and preference is always changing, you're saying build that into a proposal which says here's a preference and consent management platform you can use to determine how the company, on an ongoing basis, treats your communication.

MS. LEVIN: A menu.

MR. ADLER: Right.

MR. ALHADEFF: I think that works as long as we're sure that it covers all the needs. Larry's mom is fine. She can navigate the menu. She'll re-code it for you, in fact.

But Gary's dad -- if the menu doesn't look like what he sees at a restaurant, he's not going to be interested in it.

MS. LEVIN: Also, I think Susan mentioned that a lot of consumers may not have an awareness of the data flows, and Larry mentioned that, too, lack of awareness of the data flows and what that may mean. So, how do you build that educational effort into helping them make choices?

MR. PURCELL: Well, let's be careful on the pitch, too, because although Larry's mom might not care about her data and any breach of her data might not affect her personally because of her own values, it certainly might affect this company and its brand.

So if we're going to pitch this as being something important to their brand and differentiating their brand and therefore more of a value proposition, more attractive to the marketplace, we've got to be careful not to position it such that we say that these people can do whatever they want, because if they do and something goes bad --

MR. PURCELL: It's less the individual's problem, perhaps, than it is the company's problem.

MR. CLAYTON: And particularly if they all have Internet where they're all e-mailing each other about Larry's mom just having her check stolen.

MR. ADLER: Well, presumably there's a business goal here, right?

They want to put this infrastructure in place to make their facility more desirable for customers to live in, and make it easier for customers to buy pharmaceutical products and medical services.

You know, as Larry said there's a convenience factor here for the technology.

That goes hand in hand with the fact that it's not an isolated environment. The people living there are going to be exposed through the technology to the outside world, and they're going to have both positive and negative experiences online, and that will shape the way they view their service provider.

So, that provision of flexibility from the service provider sets a different example that can be used as -- going to Gary's point about the benefits -- the market differentiation, the way an organization markets itself, realizing that by providing broad-band, cable modem, Internet access, Golden Oldies is acting like an ISP, as a service provider to its patients, to its customers. So, what should we present?

We can talk about all the challenges the organization has to surmount, the new challenges that this technology requires them to think about, and in doing so, the new opportunities in meeting those challenges, that the technology may provide from a market differentiation perspective or from the perspectives of customer loyalty, retention, increased service provision. There are a multitude of facets that we can turn around here.

MR. ALHADEFF: I just want to highlight one question that was raised here, which I think is a very important question, and it was also raised when we talked about the fact that there might be HIPAA obligations and Gramm-Leach-Bliley obligations. You said they might be operating as an ISP. If you operate as an ISP, that is a whole set of new regulations that you are subject to.

If you operate in any way as a covered entity under HIPAA, that's a whole new set of regulations you're subject to. If you can be considered a financial institution, although they probably won't be considered a bank, they might be subject to the FTC's coverage under Gramm-Leach-Bliley. That's a whole other set of regulatory obligations.

Do we want to suggest to him limitations on his business model to keep him out of those regulatory obligations?

Gary?

MR. CLAYTON: We know they're a confederation, but we don't really understand if they're one company, if they're multiple companies, where they're incorporated. There are going to be issues about the ability to even share some of this data absent residents’ permissions and other things, unless we understand that.

Since this is an initial meeting, we need to make it clear that, one, data protection is an ongoing issue that he's going to have to deal with. It's not something he bites off all at once and that ends it.

Two, it's going to very much depend on his business goal and what's the demand within his community.

And three, there are some options he has. He can use us. He can use others. He can do bits and pieces of things.

We can work with him on partnering to come out with those ideas, but I think we have to suggest that there are some things that he's got to think of.

For example, we haven't even really covered his insurance issues, his risk issues by taking on some of these new things, and how does he get coverage. But we won't know those until we understand a lot more, which I would suggest we can help him with in the process of learning about --

MS. GRANT: Exactly.

MR. CLAYTON: -- what the customers want.

MS. GRANT: Yes. I think we need to sell him an assessment as the first phase of this, helping him assess how he's operating now, what the people who work there need and want, what the people who live there need and want. From there, we can go to step two, presenting him with the obligations that are attached to those, the opportunities, the benefits, and so on, all under the general sales pitch that the direction that he's heading in is potentially a great direction for the people who work there and who live there in terms of providing them all with better services and benefits.

MS. LEVIN: We might also want to make him aware of all the governmental resources and nongovernmental resources available to him to help educate staff. There are some free resources that they might want to avail themselves of.

MR. PURCELL: We'll charge you commission on those.

One thing that I want to make clear -- how do we pitch this? We will be going into this meeting soon.

It seems to me that -- just to throw out a straw man here -- one of the things we can do is we can essentially paint a big picture. First, say we’re very glad to see that your mind's open to this, here's how good it can get. Then start peeling that into the increments and categories we've been talking about and say, here's what to do for a foundation, here's how you build up this model that we're painting here, and this may be a a four-or-five-year deal and it may take quite a while to get where you want to go.

MR. ALHADEFF: Yes. I have a concern. I've met the CEO once, and he reminds you a little of the '60s -- he still has his ponytail and he wants to do the right thing. He thinks he's doing a good job, and he's really suspicious. He's already told us he's been suspicious of consultants trying to sell him multi-year contracts.

MR. CLAYTON: We clearly need to tell him that maybe at the end of this process he decides not to do some of this or any of this. We're all acting like this is a given, that it might be better for them, and that they all want it. He may find that it's not a solution he can afford and not one that he wants and it doesn't really give him what he needs.

So, in addressing that, we have to be open to all possibilities, both pro and negative.

MS. LEVIN: Susan's point, though, of thinking about it in terms of pieces is something I'd like you to think about.

MR. PONEMON: Just one point. For those people in the room who have been on either this side, the consulting side, or on the client's side, you know that assessment is an evil word.

No one wants to spend real economic resources on assessment.

If we're trying to sell something, going in with the assessment is going to be difficult unless there's some pain, unless that organization has experienced a problem, such as a violation of GLB or HIPAA or some embarrassment factor.

So, assessment is the right place to start, but we might have to think about doing it differently. We might have to bake it into the overall value proposition and project.

MR. ALHADEFF: Let me do a little wrap up before we run into part two. I think we've identified a number of the risk factors. We've indicated that because he's a bit enthusiastic to begin with, we don't want to start him off with the negatives. We want to pitch early to the positives.

But we're going to have to raise the negatives before we pitch the assessment, because he's going to have to figure out that there's pain if he doesn't go through this. Then, after the assessment, based on the interaction, I think we're going to have to develop a little bit of this during the first meeting as it goes along. One of the things we're going to need is to get more information than what we have and how that works. We have done a little bit of a brainstorming prior to this meeting.

And by the magic of photocopying, in your packets, there is concept piece of some slides which will include some of the challenges of privacy impact assessment, some of the solutions that may also be available, as well as some of the deployment considerations and factors.

Now we will magically morph -- Richard is going into 1960 as we speak. We will be morphing into the various role-playing positions, and I believe on the hypothetical outline, you've got the roles which we're going to be assuming for part two.

Here’s our CEO, Richard, who is --

MR. PURCELL: Hey, Joe. How are you doing, man?

MR. ALHADEFF: Good man. Dude.

We've got Larry, who is our chief operating officer.

We've got David, who is our chief financial officer.

Susan is actually director of communities.

I'm their outside legal counsel.

And we've got our consulting team -- amazing how we're split up this way -- which is Gary and Steve on the consulting side and then Steve again -- should we use Steve and Steven just to differentiate? -- Steve, who is our technology consultant guru on this deal. With that, I'm going to turn it over to the consultants, who may want to figure out the pitch, and you can use the materials as if they have the hand-outs.

MR. PAROBY: Well, to start out -- thank you for our first meeting.

You raised a lot of issues. It seems you want to go in the right direction, using technology, using enablers. Our first thought in synthesizing some of the information from our first gathering is that we certainly don't have all the answers to the questions that we need in order to go forward with what I'll call a full fledged proposal or a solution. Some of the challenges that you're going to be facing as you move into technology and move into the next era with Golden Oldies are some privacy challenges, some security challenges.

And although a lot of organizations think they know where they are with respect to their information practices and technology needs -- one of our value propositions is to consider your vision, your goals, your objectives, and your desires -- where do you want to be in six months? Where do you want to be in a year? Where do you want to be in five years?

And then map that back from your vision and your strategy to where we are today and take a look at the current state and then help you design a framework as you go forward, using any kind of enabler -- it may be technology. We need to first build the platform from where you are today to where you want to get to in that time-frame.

Now, that takes various forms. You need to involve certain people. You need to look at current regulations. You need to look at things affecting you like HIPAA laws. You need to look at the Canadian regulations, because you do have operations there, and that first initiative can be done in many ways.

You can do an audit. You can do a current state assessment.

One way is to bring in key people from Golden Oldies -- yourself, legal counsel, privacy officer, technology experts -- and actually work through that process to determine what their thinking is as far as where they want to be, where you want to be with your vision and your goals, and map that against where you are, and in a very cost-effective, short time-frame determine that current state. We can use that as the baseline to be sure that, as you go forward with respect to technology, innovation, trying to get cost-effectiveness factored into it -- to look at how you can get a return on that investment, both tangible and intangible. Tangible return means we're going to do this actually more cost-effectively, we're going to do it more efficiently, we're going to save money on purchases, we're going to grow efficiently. But intangible return is how that's going to affect the brand from a security, privacy, technology standpoint.

How are you going to be a key differentiator as you grow?

MR. PURCELL: Well, growing is everything for us. You asked, where do we want to be, and where we want to be is profitable and continuingly profitable.

One of the goals we have over five years is to grow this organization.

We have five communities here in the United States, and we just acquired one in Canada about a year ago. We want to grow both sides of the border, and we think there are some other opportunities, too, south of the border, as well.

So, we've already had a certain amount of regulation that we've dealt with, but when you talk about the chief privacy officer and the technology and everything, you're looking at it right here.

I mean this is it. We're not huge right now, but we're going to grow.

What we want to do is grow effectively and kind of slowly.

Larry is our operations guy, and my task to him is make sure everything is just as efficient as can be, and he's told me -- and what I told Joe when we met at that tech show -- we're not very efficient. We're shoving paper and disks and stuff like that to each other.

Security -- it doesn't sound very secure right now, so I'm not so sure what you're going to sell me there.

Our technology guy is our CFO, our money guy. David is the guy that does this for me -- he makes sure that the numbers add up but also that we're not running liabilities and risks beyond what we need. Joe helps him figure out that risk.

When you talk about what the community needs -- we serve a group of residents here. They're our customers, and everything we do is focused on their benefit.

Susan is the one who needs to take care of what they need.

Let's start with Susan. You respond first, because what Steven was talking about mostly is what our customers are going to want and how their lives are going to get better.

MS. GRANT: Well, the community directors for the various communities have gotten together and talked about all of the exciting things that we could do for the residents with new technology and also how we can just share information amongst the community directors better about activities and share ideas for things to do.

The potential here is so great, but what we really need to do is probably have some meetings with the residents, which we haven't done yet, to talk about these things and find out more about what our ideas and what their ideas are and what any of their concerns may be.

I know just in talking amongst ourselves, one of the things that one of the directors brought up to me is that no matter what we do with technology in terms of serving our residents better, we also have to remember that we need to offer them just as good service off-line. We can't force everybody to go online to communicate with us or to get the things that they need. We still have to keep on improving the services that we offer in other ways, too. The other thing is that we all feel like we need a lot more training not only for our residents about how to use all this stuff but also for ourselves.

MR. PURCELL: I think that's true. We didn't make this company happen. We don't establish this because people are being put away.

These people have their own lives. They're independent.

We do everything we can in this community to make sure they have their independence.

So it's really important to us that our residents get empowered with using these tools.

A lot of them already know this stuff better than some of us do, but a lot of them don't, and they share a lot with each other.

But what we found is we had a few problems. Somebody who was considered a resident expert was giving bad advice to others. What we need is a program that lets everybody get the same information and clears out a lot of the myth that has been circulating.

MR. PONEMON: As the chief operating officer, I'd like to talk about the bottom line because the CEO only looks at things from a positive side, like most CEO's.

So, from the bottom line side of the universe, let me just tell you, just within the four walls here -- we are not being videotaped, are we?

Because I want you to know we are in violation of the law right now. The good news is, because we're not networked or connected, no one really worries that much about it. But on the other hand, we just want you to know that we believe that we're in violation of all of these regulations and laws right now, not deliberately, but we know somewhere out there these laws exist. You're just going to have to help us walk through it, because we don't want to do this only to find out that we're the subject of a great investigation by the FTC.

MS. GRANT: Yes. You mentioned HIPAA. I don't know what that is.

Do you know what that is?

MR. CLAYTON: Well, you raise a couple of good points, and it's not surprising to find that you're violating some provisions of the law. A lot of companies are, either knowingly or unintentionally.

We're not legal counsel. We're not here to give you advice on that. Certainly we can help you in some of those areas.

But one of the things I think you need to look at and, stressing some of the positives that your CEO has brought up is, you clearly are involved in your communities, you clearly want to serve them and you want to do good things. One of the things that strikes me, as you suggested, is to understand, one, how you can have immediate impact by improving your own internal operations. That may answer some of your COO's problems.

How do you do billing? How do you share information? What are the ways you connect among your various communities?

And we typically talk about data flows and network design, but how are you passing information, either information about people or information about things or information about events, back and forth, and really, how do you talk?

Because what it boils down to is, it's people to people, and all we're doing is using technology as an enabler to get you there.

The second thing is you may find that things that you thought were going to be a benefit from technology may not be.

You may have to make a business decision. Is it cost effective? Is it going to help you reach your goal? And you may find that you've got to do some training not only of yourselves but of your community to clearly understand what the opportunities are and how to use it and how to impact it.

And one way to do that might be for us to work with you on understanding how to improve your own internal operations first and, as part of that, do the outreach to the community where we understand what they want, what their issues are. One of the urban myths you're going to have to address is the concern that they have about technology being a positive but also a negative. You've got the reality that, in a small community, you're much like a community bank.

While you're very close to your customers, if one thing goes wrong, it's just like your neighbor breaching a confidence.

You hurt your reputation, you hurt your community, and people will get upset with you, particularly if you made representations.

But going to Larry's concerns about privacy violations or HIPAA violations, there are a number of laws at the state level, at the Federal level, and outside of the United States that regulate how you can gather, use, share, and transmit information.

It's particularly regulated in areas where the information is very sensitive, such as health care, and if you're involved in billing or collection, or if you're going to be providing other services where you've got physicians providing information or helping pharmaceutical needs and the like, you very well may be regulated about how you can use and how you collect information, what do you have to do.

Going to your profitability issue, you clearly want to do things to cover your own risk on this. That may be something we can help you with in the process, but it means that we've got to marry the business goals that you've got, which are real, which are concrete, which are clear in your mind, with a lot of things that you don't perhaps understand that we can work with you on about how you get the information you need to make the decisions.

MR. PURCELL: Okay. So help me out with this, because we have a lot of elderly people here. They have a lot of health issues, and we have this whole list of physicians who come here. They provide services here in our clinics, but we don't keep the data. That's the doctors' stuff.

But we have access to some of the data, because if somebody has a medical problem, we have to have a certain level of access to understand who their doctor is, what their last treatment was, that kind of thing. We have some medical facilities here for medications, too, where we dispense medications.

But that’s the doctors' problem, not mine, right? I mean I don't understand how that's my problem.

MR. ALHADEFF: We haven't done this without any legal thought. We have secured the information appropriately, because there are lap-top locks on all of the lap-tops, and I think, Ivan, you've got everybody's password on your computer, just so that we know where it is.

MR. PURCELL: Yes.

MS. GRANT: And the file cabinets are locked.

MR. PONEMON: But actually, there is one other thing. We do sell information to large pharmaceutical companies. Did you know that?

That's how they're actually getting some clinical enrollment and all sorts of things.

MS. GRANT: We are? I didn't know that.

MR. PURCELL: You've got to start attending the meetings, Larry.

MR. PONEMON: Is that a problem?

MR. ADLER: Ivan, we've talked about building a health care portal for the six residents' organizations so that we can --

MR. PURCELL: A portal? What's that?

MR. ADLER: That's that collection of information on one screen.

MR. PURCELL: Oh, just a main thing? Okay.

MR. ADLER: Right. Where different hospitals and insurance companies and pharmacies and residents and physicians and patients can all communicate about the same common groups of information to streamline communication among the organizations.

And even though we may not ultimately hold that information ourselves, we're nevertheless going to be the conduit, providing discrete access through our portal, through that window, to all those different application service providers, and our customers are still going to look to us as the custodians of their data, because we're providing the access to the hospital, to the doctor group, to the insurance company, to the different communities.

MR. PURCELL: Can you find some reliable people who won't let me down, then? Because this is a brand image for me. If they mess up, then my chance of getting my seventh or eighth community is pretty bad.

MR. ADLER: Right. For us, our business is people. We build a community for people to come and live and enjoy their retirement, but from an IT infrastructure perspective, it's about data. As soon as we transform all the information we collect about people into the systems where they can gain this new convenient access to information, we now have this enormous responsibility outside of the regulatory regime, because our customers are looking to us --

MR. PURCELL: Okay. So, now you're --

MR. ADLER: -- to protect their information.

MR. PURCELL: You're telling me it can be more efficient, but it sounds like there's a big cost to that efficiency.

Is this really worthwhile? Why don't I just keep doing what I'm doing?

MR. PAROBY: One of the things we're going to suggest to you to consider as a go-forward strategy -- and I'll dumb it down. It will be really simple.

First we need to --

(Laughter.)

MR. PAROBY: Consulting 101.

You have to think in two camps.

First of all, you're serving a community. You're serving people.

What are their demands? What do they want? What don't they want from their standpoint?

These are people who may or may not want to be empowered. They may or may not want privacy and security. So, let's figure that out.

That could be surveys. That could be interviews. That could be focus groups. Pretty simple stuff.

The next simple thing is to take your goals and your vision, as we set up earlier. Where do you want to be in a period of time? What do you want to look like? What do you want your brand to be? Do you want the seventh facility, the eighth facility, the tenth? Do you want to go overseas?

Take that, with what your residents want, and map an interface with who you are impacted by -- pharmaceuticals, health care -- what regulations, what impacts them, their families, their grandchildren, whomever -- and look at a phased and structured approach, starting with the people, looking to technology to enable it, and a very simple plan.

As I said, what do you want to do versus what they want.

If you want to do something that the residents don't want you to do, it's not going to be cost-effective, and it will hurt your brand.

So, first, what's your goal? What is the residents’ vision for life as they live within your community? And take that and map it.

MR. PONEMON: Let me just jump in here. I talk to our customers.

These are elderly folks, and if they can get a coupon, an e-coupon by providing a whole bunch of their data, they love it.

They don't complain at all. They get a 20-cent or 50-cent coupon. They're willing to provide all of the personal information the pharma companies and the health product companies want.

So, I don't see any problem in just selling that information, because it's beneficial to them. Are you saying that, by doing this, we're going to take away what is potentially of value to our end customer?

MR. CLAYTON: Well, you may well have to take some of it away, to tell you the truth.

One of the issues you have is do you need to do something differently?

You recognize that there are laws that may regulate what you're doing, and the answer is why would you want to do it?

Some of the laws, like HIPAA, actually have criminal sanctions.

If you're intentionally violating provisions of the law, there are criminal sanctions that can be involved. Those can be serious, and they're enforced by the government. It may well be that you need to comply regardless of whether you move forward or not.

Secondly, you may or may not even have risk coverage for some of the things that you're talking about doing.

If there's exposure, you may not be adequately protected. One sure way not to get your seventh home or community is to get sued for what you're doing that may be in violation of the law and cause you a problem that's not covered.

MR. PURCELL: Joe, I need a briefing on this HIPAA thing, later on, okay?

MR. CHAUM: And I'm very, very concerned about the liabilities, of course, and so, I think one thing we should be doing is getting rid of all data that we absolutely have no real essential need for.

Maybe we could make a few bucks selling some in the future.

We had some vague thoughts we might be able to really analyze the data and help with our marketing or something, but this has never panned out.

So, I think we should behave like my local library.

They've decided now they want to destroy all information so that the FBI won't get hold of it. We should have a very effective program to make sure that we absolutely get rid of everything we don't need.

On the other hand, I think we should look at trying to make money off of offering some features as a choice to our residents and their visitors and maybe even to their families to communicate with them, giving them some value.

MR. PURCELL: That's cool, David, but make sure, because Larry and I really need some information to make sure we know how to structure our deals. We've got some opportunities to buy a couple of other communities coming up, and we have to know how to do that.

I don't want you to get rid of so much information that we get stuck and I can't even go forward.

MR. CHAUM: We'll just keep it in the aggregate.

MR. ADLER: I just want to say, as a technology advisor, that when we build this portal, it's a two-way street.

On one side, we're going to collect a lot more information than we've ever had before, because electronically, we're going to give people the ability to submit more information than they've ever been able to in the past.

And that means that we are going to have more people from more places accessing more information faster, easier, cheaper.

That's going to be good for the brand, because that's going to increase, through word of mouth and on the Internet, the opportunities for our business to grow and expand.

This portal will become an advertising platform for the company.

On the other side, we've now got this new security and privacy requirement, because we've got to make sure, for all those people who are submitting information, that they're only submitting the right information and that only the right people are gaining access to the right applications and to the right data for the right reasons.

We have got to keep track of all of that, because we do not ever want it to turn out that the portal we created to allow people to have access to more information allows the wrong people to access the wrong information at the wrong time, because that will blow up in our face.

So, we have an opportunity, but we also have a challenge.

MS. GRANT: It strikes me that we really need to look at what we do.

I wasn't aware that we were marketing that medical information. I'm not sure the residents really understand that.

I'm thinking about another program that we run. It's the find-a-book program, where the residents tell each of the community directors what books they're interested in having in the communal library, and then when we go to flea markets or tag sales or used book stores, we pick up those books inexpensively and put them in the library. We've got file cards in each of the offices with the names of specific people that have recommended specific books.

But it seems to me that if we were to put all this information online, maybe we would want to step back and think about do we really need the names associated with specific books or could we just post to everybody the fact that we have added new books to the libraries without having it linked to actual people?

I'm starting to get nervous when I think about all the information that we have about the residents and what they like to do and so on, and I'm not sure that everybody wants to share that.

MR. CLAYTON: Just a comment.

What we're doing is struggling with one of your major assets, information about your people, and how do you use it. You wouldn't simply start throwing away other assets without doing an assessment of the cost, the risk, the need, and the opportunity associated with it. Until you fully understand the impact that getting rid of information or collecting information or not having it will have on your business, there's no way you're going to effectively reach your goals.

That may be an integral part of your business. You've got issues about employees and how you're using and sharing information, how you're collecting it, and those have to be married.

I'll tell you one thing. You'll never reach the goals that you're seeing of seven, eight, nine or growing across the country with communities unless you fully understand the data flow issue, because it is a valuable asset.

You may be aware that, 10 years ago, most of the wealth of companies was from fixed assets -- brick, mortar, and things.

Today it's technology or information. It's intangibles.

You may find that the thing that makes you the best company is what information you have on your community and the ability to use it, and you may well be able to effectively transfer that information to companies by simply going through the correct process of doing it.

So, don't take literally some of the general comments today that you can't do these things.

You've got to look at your data flows. You've got to map it as part of your business. And it's just as essential for you to understand it as a CEO as knowing your money flows. If you want tight control over your money, you'd better follow where your data flows about your individuals, your employees, and others.

MR. PURCELL: So, who does this right?

I mean I'm just a small player here. Who's good at this?

MR. ALHADEFF: I've got a pretty uneasy feeling. I went on the web and looked at their website, and they've got a slick presentation which I don't think we should be paying for. They have this whole thing about different technologies and it's got this bull's eye thing on it. I look at that and I think about Cousin Zeke who runs the facility in Arkansas. He doesn't even understand some of those words.

MR. PURCELL: Talk about marrying data.

MR. ALHADEFF: How do you guys see us doing all this stuff? I mean spam blockers, SML, whatever that is.

MR. PURCELL: I know. What is this stuff? This looks pretty complicated.

I mean we're just -- we're a small group.

It's Darryl and his brother, Darryl, right?

(Laughter.)

MR. PONEMON: Here's the deal, okay? The deal is that we're talking to three other companies, and they will do all of that up-front work for free as long as we buy their technology solution.

You talk about all the benefit and value. If you can demonstrate the value -- so, we give you a dollar and you give us two dollars back, that's valuable. We'll split that two dollars with you.

So, would you ever want to work on a contingency fee basis so that you prove the benefits and we pay you? Because one of your other competitors is actually thinking about doing that.

MR. ADLER: Well, not only that, but I would say if you take a look at the issues that were identified in the privacy impact assessment charts, where it identifies from a privacy and security perspective, all the areas that we have discussed that impact your business, it is pretty exhaustive. If you were to try to do this without technology, just with manual policies and procedures, you would be talking about a consulting engagement that certainly would not be pro bono. It would be fairly lengthy. And from an overall operational management perspective, it would be extremely expensive.

So, the cost of the technology investment will be more than offset by the process automation, by taking all of these areas of human interaction, manual procedures, policy enforcement, and building that into IT systems so that human beings don't have to remember it.

And just like we're going to use IT systems to automate our business so that we can expand and increase efficiencies and communication, we want to use the same technology to enable and control the effective and responsible use of information, because we realize from a business perspective that we can't continue to operate in a purely paper-based environment today.

There are these huge efficiencies we can obtain by automating, and that holds true for privacy management, as well as business management.

MR. PURCELL: Well, I'll agree with that, because David and I have been talking a lot about what we're going to do in terms of expanding. We're even talking about can we go public any day? He's told me there's no way we could ever go public given the infrastructure that we've got built today. So, it's between David and Larry here to figure out what's first?

What I've asked them to do and what I want to know from you is what's first. I can see all this, but it looks like analysis paralysis. We could be six to 12 months just sitting here doing assessments, and that doesn't change anything.

MR. ALHADEFF: Unfortunately, we're at a point where you are saved by the bell on analysis paralysis. We're at a point when we do want to give an opportunity for some interaction with the audience.

I want to point out that we've taken a hypothetical that marries more issues than any one company is likely to be facing at any one time.

We've given them, unfortunately, a well-armed and ornery officer staff to give the consultants a bit of a hard time in terms of what they're trying to pitch. But the concept here is the solution has to be holistic. It's not out of anybody's reach, but it's something that has to be done first by understanding what your data flows are, then by doing a phased analysis of how you get from point A to point B with the needs of the company and the needs of the users both in mind as you go forward.

So, the end note for our part, before you start to ask your questions, is that technology helps, but you've got to sweat a little, too. The problem is significant, but the solution is doable.

And with that, why don't we turn it over to you for some questions? There's a mike in the back of the room.

QUESTION: One thing hit me in the middle of this role-playing.

Larry mentioned people who are quite happy to give away private information about themselves in return for a 50-cent coupon.

So, I was asking myself what is that information really worth, and I realized I have no idea. What is the real value of that private information?

MR. PONEMON: There's not a lot of hard data. The data that exists about how companies monetize information -- the research is spurious, and there's a lot of variation. But there are some studies that suggest that this information is valuable, and it depends on its application.

For example, medical data is deemed to be more valuable than, say, financial data, because it's just harder to come by, and companies like to use it in the product testing, clinical research. CRO organizations, pharmaceutical companies, might actually pay a handsome sum to have more reliable information.

See, it gets back to the basic value issue that Steve was talking about.

We worry about opt-out's -- we have breakage or we went from an 80 percent to a 60 percent, but that's a good fact, because you now know that 40 percent of your population don't want to get a message from you for marketing purposes.

So, the better the information about the customers that are interested, the more effective you are as a company in meeting your revenue and marketing and sales goals.

In answer to your question, there’s a lot of talk about how valuable this information is. I just don't see a lot of hard data supporting that value proposition. But I know it exists. It does exist.

MR. ADLER: Of course there are numbers about identity information in the black market.

It depends on who is buying the information.

There was that article in December of last year in which some Long Island companies had somebody steal 30,000 identities, and it was sold for $2 1/2 million.

MR. CLAYTON: And you can look at some of the case law, even the FTC and some the cases they've seen. You can look at the value of what people were willing to sell, some of their data on their customers, particularly financial institutions, some of the early cases there. People got a lot of money for selling it.

But I will tell you the value of the data is going to depend upon what is the supply, what's the demand. It's basic economics in one sense, but it also is going to depend on what you can do with it legally.

We were hired after the fact, but a large retail organization decided to buy a large company out of the country, and they paid a large amount for it.

The company was the largest holder of information about citizens in that country.

Lo and behold, that country had data protection laws, and they couldn't export the information and basically couldn't use it without specific opt-in permission. As a result, what was potentially very valuable information was basically worthless, and they overpaid for it.

So, to me, it's just typical business analysis issues. I don't think there are hard-and-fast rules and studies about it.

For each business, if you walk through the elements of it, you can come up with a pretty good understanding of the value of the information to your organization even if you can't quantify it specifically.

MR. ALHADEFF: I think you also have to realize that there are two value propositions. There's the value to the organization and the value that the subject, the consumer, would put on the information, and that will vary by country and by culture.

It's probably possible to establish a value proposition in the U.S.

You're probably further away from establishing that in certain parts of Europe and certain other parts of the world, just because the concept of trading information is either less accepted or less common. So, there are issues that are going to come in there.

Don't just think of the value to the company. Understand that there's a value to a customer. And if you want the sharing, then you have to give the appropriate incentive, whether it's that you prove legal compliance in some fashion or whether you give a financial remuneration of some kind for providing the information.

MS. GRANT: And it's not just whether or not there is financial remuneration for the consumer.

In order for the consumer to figure out whether it's worth trading this data for 50 cents off something, the consumer really needs to know what it's going to be used for and by whom.

MR. ADLER: And who it's going to be protected by, because again, I go back to the identity theft case, where there's a black market for an identity, and somebody may be willing to pay 60, 100 dollars for what may be used for fraudulent credit cards. But then that's only the first transaction.

It's when the fraudulent credit cards are created and your ultimate credit rating, perhaps, is the ultimate determination of the value of the data.

MS. LEVIN: On June 18th the FTC is holding a workshop on the costs and benefits of data flows. This information will be coming up then, too.

So, let's move on to the next question, and we'll have some more information on the ones you've been asking at the June 18th workshop.

QUESTION: This is just a bullet point that was on your outline, and that is California Senate Bill 1386.

Could anybody talk about what you would have advised them to do on how to get ready to comply with that?

MS. LEVIN: We probably don't have time to answer that. I'm sorry. But if you care to talk with one of the panelists afterwards, perhaps they can give you some guidance.

QUESTION: And the other question is -- nobody really raised the issue of Golden Oldies using behind-the-scenes technology like web bugs and what you would suggest that they might or might not do with that.

MS. LEVIN: You mean technology they can put on the computers for their citizens to use?

MR. PURCELL: Yes. We didn't address that.

QUESTION: And gather information.

MS. LEVIN: Oh, I see.

MR. PURCELL: We didn't address that largely because we're not doing that at this moment. Golden Oldies hasn't yet deployed that -- but it's certainly one of the issues that they'd have to address as to what data they're collecting that's personally identifiable and that collection is known to consumer but also, importantly, what data they're collecting in an unknown and undisclosed way. That's very, very important to do.

MS. LEVIN: We're going to run a couple minutes into the break and shorten the break up a little bit, because I do want to get to some more of your questions.

MR. CHAUM: Let's not forget the other costs of the data, the risk that it might be abused.

So, you have to weigh that in the cost. Then there's the financial risk. There's damage to the brand and so forth.

There's also the cost that you incur by not being able to say definitively that you don't make certain uses of the data, and that might help you.

MS. LEVIN: Next question.

MS. PERRIN: I know there's a line-up behind me, so I won't do the full scenario, but I think you're a bit modest.

You said you made it complex. You left out one element that I think makes it even more complex. Let's imagine I'm Mary Paininthebutt and my mother, Jane Snowbird, is in your home in Florida and I'm up in Montreal, right? And I have power of attorney, so I'm managing her finances, and I'm managing her health stuff, because she's 85 and she needs me to read her diabetic read-outs and all this. You haven't got a secure facility, and we tried using diskettes, but they kept getting opened at the border by Homeland Security.

So, finally, I had to go to other methods to get that data.

We tried faxing, too, but that isn't secure. It's even less likely to be.

So, I went to your home in Victoria while I was there for a conference and I got one of the computer geeks that's working in the dining room -- nobody in the office knew how to run the system -- and lo and behold, he can get everything and yanked it up to BC. I'm so fed up by now, because my mother is scared and she wants to move home, and I'm saying don't worry, we'll complain, we'll get this all cleared up.

So, I've just filed a complaint into the BC privacy commissioner, because once I yank it up in BC, it falls under that jurisdiction.

MS. LEVIN: Stephanie, come to panel two after the break, because we will be looking at some of the answers, how technology can help.

MR. CLAYTON: And we're going to turn you in for unauthorized access to our computers.

MS. PERRIN: Oh, it's all legal. It's all legal.

But the element here is that the families are the ones managing a lot of this data, not the guys in the home, and they're the ones that are going to complain.

MR. PURCELL: I took a note, but we didn't get to it, about where is the authentication and authorization procedures for data access internally to the company, but we didn't get to that.

MS. PERRIN: Well, I'll bet you anything it's whoever knows how to do it, and that's the computer tech kid in the dining room.

MR. PURCELL: But that's how it would be today, yes.

MR. ALHADEFF: And one thing that we didn't want to delve into, which is actually something that would address some of your issues, is what's the legal and contractual infrastructure between the residence communities, the residents, and the administrative staff, because some of that will be spelled out, and then what are the internal policies that give permissions.

Part of the problem is this is a group that didn't have those internal policies.

So, it's not even just that the technology didn't reflect it. There wasn't a policy to begin with, which is even worse.

QUESTION: Mine is more of a concern, and you can address it in whatever free form you wish. It seems to me a lot of the issues here are very, very premature, that there's really a shaky foundation, and there's some fundamental corporate governance issues that need to be resolved before you can even get to these stages, like does the corporation have a code of ethics, and how does that govern how they conduct themselves? How do they monitor their code of ethics? How would you advise them to address those fundamental cultural and legal issues, their corporate governance?

MR. PONEMON: Can I just chime in, because actually -- I didn't pay this man to ask that question.

MS. LEVIN: I thought you did, though, Larry.

MR. PONEMON: Not yet.

MS. LEVIN: Sounds like it.

MR. PONEMON: But it is all about ethics.

Unfortunately, we jump into the compliance and regulatory issues, but it's about responsible information management.

We talk about all of these bad companies, but companies are filled with good people, and they're trying to do the right thing.

They just need clarity of purpose. They need to understand that it's about responsible information management and not just about something narrowly defined as the privacy thing or the data protection thing or the Canadian -- the PIBIDA thing once we get into that mind-set, it's gone.

It's confusing to most people, and we move on to the next issue.

So, I agree completely, it starts with this ethical respect for a framework that makes sense and that could be applied globally, and then you could start to work at the next level of detail about how do you comply with that framework.

MR. CLAYTON: And part of what you're raising and the data flow analysis -- you'd go through those issues.

Those are things that we clearly would have to understand, because the analysis of what's collected, where it's collected, is it legally collected, what are the risks associated with it, have got to be understood at every juncture of the process. What I would hope a company would get at the end of this initial assessment or analysis paralysis would be a very useful diagram flow, risk report, et cetera, that walks business through almost all of those issues and offers either solutions or at least choices or where you can get other information to make those decisions.

MR. PAROBY: I said I'd dumb it down and make it simple, but one of the things we're seeing in very large organizations and very small organizations -- Larry hates the word "assessment"; I'll say "current state" -- is to issue them a scorecard on their current state, a very simple scorecard, and we've coded it red, yellow, green, to make it simpler yet.

Red is bad, green is okay, yellow is maybe I don't know or in the middle.

Once you establish the ethics, the culture, the framework -- and this all goes across technology, the people issues, the corporate governance, the privacy. You sit down and you look at that at even a board level and you say, gee, I've got a scorecard, and I'm red over here with respect to these ethical issues or -- let's address those first before you implement a solution with technology.

MR. ALHADEFF: One of the things that you have to think about, especially with smaller companies, is when they start an analysis like this, what you may end up having is a forcing function, because there may be a code of ethics that is actually -- Ivan is the code of ethics.

It is actually the CEO who has the ethos of the company. We actually have a fairly large company considering what a lot of companies actually are, and the code of ethics and a lot of these policies may be things that, if you ask someone, you could get an answer, but if you were to look for it written down in an institutionalized fashion, you'd never find it.

MR. PURCELL: Well, it would be insulting, too, for a small company, to go to somebody and say you need a code of ethics. I'd say, get out of here. I mean you're assuming I don't have ethics.

So, it's in the very, very large companies that have really distributed accountability where I agree that the documentation is more important, but you've got to be careful when you're dealing with the very small, closely-held companies, as well.

MS. LEVIN: Okay.

Next question?

QUESTION: Actually, to pick up on the small company issue, at Trasue, we see a lot of companies who have no understanding of things like CABA and other kinds of regulations that are specific to their own state. The lack of understanding, especially among small companies, of applicable law is a big problem, and I think the FTC and everybody has to find a solution to that.

MS. LEVIN: More Education 101.

Last question.

MR. REEDER: Sure. And it's pretty basic. And that is what is the definition of privacy for you as the CEO of this company?

MR. PURCELL: Thanks a lot, Frank.

(Laughter.)

MR. REEDER: From the sense of what privacy is and what your sense of the expectations of your customers and the world at large about what privacy is, doesn't that draw the line for you as to what protections you provide and how you go about putting your arms around what you should be doing. Because, on the one hand, FTC is dealing with, and Congress is dealing with, the spam issue, and the do-not-call list is about to come out enabling people to do that, lots of work is being done in identity theft.

For some, that might be enough as far as kind of the privacy intrusion part of it, but isn't there more to it than just that?

MR. PURCELL: Well, I think that blends the prior question on the ethical framework, too, Frank, because I think Ivan Offerforyou is essentially being advised to do a survey and to gauge the attitudes toward privacy and data protection in their client base. That would not necessarily be a voting process to determine an outcome but would rather be an advisory into that ethical framework to say, okay, fine, this is what people expect. Now what am I going to provide within that expectation that's required through regulation and that goes above and beyond that needed for brand, that endures to the brand somehow.

So, I think it's very complicated to say how you define privacy.

Certainly, Larry's mom is going to define privacy in a very different way than either her peer or my high school student who I'm still trying to convince that stealing music on the Internet is not a good thing.

So it's very difficult to say here's a definition.

I think that it's self-defined, to a certain degree, even in legal terms today.

MR. PAROBY: There's an exposure draft that just came out yesterday. It's by the AICPA, and it's entitled "Proposed AICPA CIC Privacy Framework," and they define privacy. They say privacy is defined as the rights and obligations of individuals and organizations with respect to the collection, use, retention, and disclosure of personal information, and they take each of those major components and they re-define that.

So there is finally a framework, 90 pages in length, that is starting to at least define it and give some guidance as to what it is and what you do with it and what you can't do with it.

MS. LEVIN: We'll probably hear a little bit more about that later today.

I want to thank this panel for one of the most creative presentations I've ever participated in, just fantastic.

(Applause.)

MS. LEVIN: And we're going to have a short break. I'll give you seven minutes, till 10 of. There's 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.)

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

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 in this panel. In particular, we're going to discuss current and emerging frameworks for protecting consumer information.

As you'll see shortly, there's a wide variety of approaches here.

We have both regulatory and voluntary.

We have very highly technical and also high-level principles.

You'll hear first from each presenter a very brief overview of a particular framework.

Then we're going to move into a broad panel discussion to explore the commonalities among these frameworks, the barriers and incentives to implementing the frameworks, and whether and how we hold businesses accountable for implementing the frameworks.

I'd like to first introduce to you the panel.

From my far right, we have Larry Clinton from the Internet Security Alliance.

Next to him is David Fares, U.S. Council for International Business.

Laura Lundin from BITS, the Technology Group for the Financial Services Roundtable.

And here, even though you can't see him yet, is the one and only Mark MacCarthy from Visa.

Next to James is Fran Maier from TRUSTe, Frank

Reeder from the Center for Internet Security, and Laura Berger, an attorney with the Federal Trade Commission.

Larry, I'd like you to open, please.

MR. CLINTON: Thank you very much.

I have promised Loretta that I will do this in five minutes or less, so if I finish mid-sentence, just let me know.

I'm Larry Clinton with the Internet Security Alliance.

I want to let you know, first of all, who it is that we are.

The Internet Security Alliance was created about six months prior to 9/11 because the folks at the CERT Coordination Center, which, for those of you who don't know, is essentially the fire department for the Internet. They do all the really hard-core, geeky threat vulnerability analysis. They combined with the Electronic Industry Alliance, because CERT was primarily getting this information to the Federal Government, and the private sector, as we know, operates about 90 percent of the Internet.

So, that's what the Internet Security Alliance is supposed to do.

This is a list of our board of directors. A couple of quick comments about that.

We are aggressively international. We are non-NISEC in the sense that we do not operate within domestic cylinders. We are also aggressively inter-sectoral. We have AIG Insurance. We have Visa and Verizon. We have Nortel Networks. We have TATA from India, Sony from Japan, C&W from Britain, et cetera.

This is the Internet. We all recognize this. I remember the Internet when this was first put out in 1980. Everybody thought this was very complicated. How could we possibly deal with that?

This is the Internet today, which is a little bit more difficult to deal with.

Last time I was here, I noted that that really intense purple area is the FTC. I've been told that it is not. Actually, that's my daughter downloading music.

What is interesting here is the trend line. Despite all the attention that we are giving security -- and you've seen a lot of technologies that have gone earlier today -- the trendline for security incidents is straight up through the top. Incidents and vulnerabilities are increasing 500 percent a year.

So, what we are advocating is that we come up with a system.

There is no magic bullet. There is no single technology. You have to have an entire system.

We advocate investing in cyber-security, considering risk mitigation. One of the things that we're going to be talking about today is new initiatives and whether or not the national strategy provides enough of these new initiatives.

One of the things we do with the Internet Security Alliance is we have a deal with AIG Insurance, the largest provider of cyber-insurance. If you become a member of the Internet Security Alliance and subscribe to our best practices, we will lower your insurance rates 15 percent.

We are trying to provide a market-based incentive program.

Mark MacCarthy is one of our members at Visa. Visa has a similar program. If you want to use a Visa card, swipe a Visa card in a store, you have to have a certain level of security.

What we're trying to do is come up with market-based incentives, because the traditional regulatory models won't work.

You can't use an FCC-style model where we're telling everybody in public comment what's around. You're then providing a road map for all of the nefarious people. You can't come up with a three-year program to provide regulatory structure, because by the end of it, the Internet's entirely changed. If you do it in the United States, it doesn't help you internationally. We need a new model.

We also think that people need to become involved in the policy debate so that we can consider this.

We also strongly advocate the adoption of best practices, and we have a list of them that I'll provide you in a moment.

These have been endorsed by TechNet, U.S.-India Business Council.

We are trying to export these.

We, frankly, don't need to write more new best practices right now.

What we need to do is start implementing them, and we strongly advocate joining an information-sharing organization. Only if the information is shared between operators of the Internet and the vendors are we going to get anyplace.

The Internet Security Alliance operates with the CERT data.

We put out these best practices. We attempt to get people involved in them, and then we provide economic incentives if they will adopt them.

Here is a list of the best practices. They're available on our website. I also have hard copies available, if people want to look at them here today. Here is what we go through in terms of our education and training.

Again, we try to provide at discounted rates the best possible training coming out of the CERT Coordination Center.

Not only do you need to have a policy, not only do you need to have practices, not only do you need to have technology, you need to have things that are going to make sure that people use the technology.

The comments made before about the wooden doorstop in the previous panel I thought were very excellent. That's exactly what we have.

It's irrelevant if you have a great password technology and everybody is still sticking their password on their computer so they can remember it. We need training for everybody.

This is a copy of the special communications that we provide through the CERT Coordination Center.

For time purposes, I won't go through it any further.

Again, if anybody has any questions for me, please contact us.

Our role is to try to expand the security perimeter in a market-based fashion, and we're looking forward to and very grateful for the help that we've had with the FTC.

Thank you.

MS. GARRISON: Thank you very much, Larry.

David.

MR. FARES: Thank you.

I'm just going to remain seated. Can everyone hear me?

Okay. I'm going to focus my initial remarks today on the work of the Organization for Economic Cooperation and Development, which is a grouping of the 30 most industrialized economies in the world. The organization is located in Paris.

My organization, the U.S. Council for International Business, is the U.S. affiliate of the business and industry advisory committee, which is the constitutionally chartered voice of business in the OECD.

The OECD recently issued a revised set of security guidelines.

The guidelines were initially adopted in 1992 when systems were largely closed.

They realized, in the built-in review process, which is scheduled for every five years, that they probably needed to be updated to take into consideration the shift from closed networks to open networks.

Luckily for me, the OECD guidelines and our work is not highly technical, because I'm not a techie.

So, I'm able to meaningfully participate in the work that we do.

But the OECD guidelines coined the phrase "promoting a culture of security." The person that asked the last question before the end of the last panel was talking about the fact that consumers don't know enough about security and that we need common-sense security.

That's exactly what the OECD guidelines attempt to address.

In very simple, plain language, it states that every participant in the information society has to assume a role appropriate to them to promote security. Awareness of security issues and responsibility are elements of the OECD security guidelines.

So I would recommend that all of you take a look at the OECD guidelines. As I said, it's not a technical document but, rather, a document that frames how every participant should analyze what their responsibilities are and what their engagement should be in promoting a culture of security.

You can access the guidelines at www.oecd.org.

We are working to help promote business

implementation of those guidelines.

To that end, we held a workshop in conjunction with the FTC where Commissioner Swindle spoke, inviting cross-sectoral industry associations to promote a culture of security with their members, and we were lucky enough to have Larry participate in that workshop.

We are also expanding upon the OECD guidelines.

We are developing BIAC, along with the International Chamber of Commerce of which we're also the U.S. affiliate. We are developing a business checklist, a business commentary on the type of questions that executives should be asking their IT department, so that there is top-level support, as well as bottom-up approaches to security.

And then, a next stage of our work will be to develop a checklist for small and medium-size enterprises and companies in the developing world. Again, it's not going to be a set of best practices but a series of questions that these types of companies should be asking themselves when they're developing their security policy.

We also have on our website links to many different resources for security that businesses can utilize.

We have a link to the Internet Security Alliance's documents and to other documents, and our website is www.uscib.org.

And with that, I will stop.

I've left some information in the back for you which gives a summary of our draft business commentary. It should be concluded by the end of this summer, and at that point, it will be accessible from our website. I won't bother giving you the ICC and BIAC websites. It's in the document on the back table.

Thank you, Loretta.

MS. GARRISON: Thank you very much, David, and I hope that all of you in the audience have checked out the materials that we do have on the table, because there's a lot of additional resource material for you.

Laura Lundin.

MS. LUNDIN: Thank you. Thank you, Loretta.

I am with an organization called BITS. BITS, for those that don't know, is the technology arm for the Financial Services Roundtable.

We are a business and technology strategy group, working on a variety of issues for the financial services industry.

Our primary membership is the 100 largest financial institutions in the U.S.

As you might imagine, this group is very sophisticated when it comes to information security, and it's often thought of as leaders in this area.

Part of that is driven by the regulatory environment in which we operate.

However, the two frameworks that I want to bring to the table today are some things that the industry has worked on through BITS, and it really addresses the products and the services that are used by the industry. The industry realizes that, as strong as its policies and its procedures and the technologies that it uses in the information security world are, it doesn't stop there.

It has to go beyond its boundaries, and it really depends on the vendors and the products and the services that it uses.

On the products side, we have started a product certification program.

This program is three-plus years in the making. We have corralled the industry to develop consensus-based minimum security features that it is going to look for in the products that it buys.

Most recently, we've harmonized this program with the government's common criteria certification program. So, now a vendor going through the common criteria certification effort can also meet the requirements that the financial services industry has set forth.

On the services side, we have developed a framework for technology risk management of service providers. Out-sourcing is being used more and more in every industry, including the financial services industry. What we've found is there has to be, again, a common set of security policies and procedures that are followed by the providers of the services to the industry.

Our framework addresses security from everything from the decision to out-source to the RFP process, the contracting, the insurance process, ongoing management relationships.

That framework is currently being updated right now to address some specific issues around security assessments, the more specific issues dealing with cross-border out-sourcing, out-sourcing to international organizations, as well as some additional measures around business continuity. Of course, this framework actually came out just around the 9/11 time-frame, but now that's obviously an area that has to go back and be revisited.

Both frameworks, the requirements that create both of these programs, can be found on the BITS website. They are public documents.

The web site is www.bitsinfo.org.

I also have a one-page hand-out outside that specifically talks about the production certification side of the house.

MS. GARRISON: Good. Thank you very much, Laura.

Mark.

MR. MacCARTHY: Thanks very much.

Let me tell you a little bit about the Visa card-holder information security program.

In the first instance, these are a series of requirements that have been developed for Internet merchants and processors, but it's important to remember that they've been a requirement of the Visa system for a long time -- that those who handle card-holder information do so in a secure fashion. A couple of years ago, we made those requirements more specific through the card-holder information security program, initially for the Internet. I want to tell you a little bit about why we started with the Internet.

Basically, it's because it's a new channel, there are new risks, and there's some brand issues related to the use of Visa cards on the Internet. But it's also important to remember that CISP, the card-holder information security program, is moving beyond the Internet.

It applies now to all entities who touch Visa card-holder information, and eventually, CISP is going to apply to all payment channels, not just to the Internet. But we started with the Internet because it was a new channel for Visa.

It's a growing part of our overall electronic commerce.

It is 6 percent, almost 7 percent, in 2002, of our overall sales.

It's up from 4 percent in 2001 and 2 percent in 2000, and payment cards are used to make most of the sales on the Internet.

Check and cash in the real world account for abut 60, 62 percent of all sales. They're not a very useful method of payment on the Internet.

So, Visa gets a substantial portion of the sales on the Internet.

It's an important new channel of commerce for us.

There are new risks associated with the Internet. There's a perception that the Internet is not a secure place to shop.

Ninety-two percent of consumers are concerned about online security. Sixty-three percent of them are very concerned.

And the reality is that many online merchants retain card-holder data in a way that's accessible from the Internet.

Fraud, as many of you know, is higher on the Internet.

So, there are new risks associated with that new channel of commerce, and that created some brand perception problems for Visa. We did not want the perception to be created that Visa was not a secure method of payment.

For those reasons, we decided to move ahead with this card-holder information security program.

For those of you who want to find out more of the details, there's a packet that I've left at the information table that will give you a lot of the specifications in more detail, but the CISP program starts with 12 basic security requirements.

We developed these in conjunction with the security experts and with the merchant community. They've been effective since May of 2001.

Let me just give you a flavor of what they are. They're very high-level.

Install and maintain working firewalls, keep security patches up to date, protect stored data, encrypt data when you're sending them across public networks, and use and update anti-virus software.

We've also developed an audit program to make sure that people who are subject to the CISP program actually are complying with it.

We've created a defined and consistent testing procedure for independent validation of these requirements. We have a list of 30 acceptable independent security assessors.

For the top hundred merchants that account for about 70 percent of all of Visa's Internet volume and for various service providers that provide service to Internet merchants, there's an annual on-site independent validation that has to take place.

For smaller merchants, there's a web-based suite of tools that they can use that will give them an online risk assessment, a self-assessment, and they go through online vulnerability scans.

Our enforcement mechanism -- there are penalties for failure to comply.

Of course, there's a period of time where we're trying to move merchants into more and more compliance. We provide them with help on remediation efforts, but there are substantial fines that can be pretty dramatic for particular companies in the case of egregious failures to comply. Penalties can include expulsion from the Visa system.

The advantages for companies in complying with this -- obviously, failure to provide adequate online security is a business risk. For some, it can be fatal.

But beyond that, there's an insurance discount. For those merchants or entities that hold Visa information and that are compliant with CISP, some insurance companies like AIG will provide a discounted premium for cyber-insurance.

How are we doing? Virtually all of the top hundred companies are in compliance today. The smaller merchants are coming along well, as well.

We're expanding the enforcement to include third-party service providers, processors, web hosting companies, and so on.

It's going to take us months to really roll out that new enforcement mechanism, but the end result -- and let me conclude with this -- the end result is that if third parties are not CISP-compliant, they will not be allowed to touch Visa card-holder data. That's going to be the ultimate way this program is going to be put into place.

MS. GARRISON: Thank you very much, Mark.

I'd like to turn to Fran Maier.

Go ahead.

MS. MAIER: Thank you, Loretta.

Many of you know that TRUSTe is the leading online certification and seal program on the Internet. Our primary purview is over privacy. Of course, privacy does include and require security, and we have some guidelines along those lines, as well.

Our consumer position is about giving consumers choice. Our tag line is "Make privacy your choice," and there's two aspects to that. One is actually providing the means for consumers to have choice about the sharing of the personal identity and information, and also telling the consumer that they've got to take an active role in ensuring that they protect their privacy and don't give it away.

Our mission, then, is to enable trusting relationships between organizations and individuals based on respect for personal identifying information.

We have a set of core privacy principles outlined in our program requirements and in our license agreement. All of the 1,200 to 2,000 companies who join the TRUSTe program have got to abide by and agree to those programs, those principles, and they follow along with the FTC fair information practices.

So, for example, under notice, they have to have a privacy statement, and it has to have the TRUSTEe seal on it.

They have to say how they collect information, who they share it with, under what circumstances it might be shared.

They've got to talk about cookies, beacons, and other kinds of things.

They have to say how they will notify users of a change in the privacy policy and a range of other notice requirements.

There's choice requirements, and probably the significant point there is that if you're going to have sharing for secondary purposes or with third parties, you have to provide user choice, at least an opt-out.

There's access requirements in terms of giving the consumer an opportunity to correct, to change their preferences, for example.

There's security requirements, and right now they're fairly basic. We're looking forward to working with industry and some of the players here today to try and provide some guidelines to our licensees about the best security.

The simple things that we ask for now are that things like credit cards be under an SSL, that there's password protection for personal identifying information, and so on. We're working now to develop some more robust guidelines in response to what we're seeing all around us in terms of the need for security.

In addition, companies have to enter into a license agreement with us, pay us some substantial funds, especially if they're large, agree to undergo monitoring, as well as dispute resolution processes, and agree to the termination requirements that we have.

And I'll tell you, we recently figured out about 10 to 15 percent of the companies who apply to TRUSTe and fill out their self-assessment and their license agreement and give us a check -- 10 to 15 percent do not make it through the process. For the most part, it's because we find that they have issues with implementation of the choice requirements or they have issues related to the children's online privacy protection requirements. That's a fairly substantial number. Of course, if they don't come into compliance, they're not available to be renewed, and of course, they don't get the seal.

And I just want to speak quickly about how we monitor. There's been a lot of questions about this over the years.

First of all, we do have dispute resolution services. This year we're tracking close to 5,000 consumer complaints now.

Some of those don't have to do with privacy, per se, but they do look to TRUSTe to put in a complaint.

We've worked with Watchfire. We're working with Watchfire now.

We've scanned about 300 of our sites.

We just started this early in the year. We're looking for things like placement of the TRUSTe seal, whether or not they're collecting cookies, if they've changed their privacy statement, all kinds of things that give us and our compliance team a chance to have a second look. We have found that 57 percent of the companies have passed, which obviously means 43 percent have failed at our first review, and some of these are not egregious problems.

Some of them are just a matter of simple fixes, and we're getting good response to that, and I think it's good for everybody.

We also do a fair bit of seeding, where we join websites, provide information, and we also go to the press and FTC, potentially.

And so, again, in the future, we want to work on the security guidelines. We're looking at a lot of activities and best practices around e-mail, and we're looking at more and more technology to apply to this area, because Watchfire has made us much more efficient, much more effective in monitoring. We think that there are other technologies, even some that we've implemented ourselves, that are proving to be both efficient, effective and strong, and that's where we're going.

MS. GARRISON: Thank you, Fran.

Frank.

MR. REEDER: We have been told that we will have a hammer thrown at us if we are not finished in five minutes.

MS. GARRISON: Or a water pitcher.

MR. REEDER: Or a water pitcher.

I guess I would like to start by asking you a question, picking up on something that came up in the previous panel. How many of you, if you're buying technology, are interested in buying technology that has all kinds of back doors and means of access, some of which you don't know about?

I don't see any hands. Well, that, in a nutshell, explains why the Center for Internet Security came about. About two-and-a-half years ago -- I guess we're all in the same time-frame -- we convened a bunch of folks to address that set of issues, and out of that came a concept, based on a couple of very simple premises:

One, that most of the damage being done, according to the industry watchers, people like Gartner, was being done exploiting vulnerabilities -- technology vendors refer to them as features -- that were known to exist and for which the remedies were widely known.

So, the problem here was not that we needed to do new research. The problem here was more of an information dissemination problem.

And the problem, really, as we saw it, had two distinct dimensions. One was -- and here I steal the wonderful phrase that Toby Levin taught me some months ago -- we needed vendors to begin to build security into their products, what Toby refers to as baked-in security. But even that isn't going to be sufficient, because most of us operate technology that is from six months to three to four years old, and data actually show that we're keeping it longer than we were even as much as two years ago.

So, we have an increasing problem with a large installed base of vulnerable technology.

The Center decided to focus on the technical detail. That is not to suggest that policies aren't important. That is not to suggest that user training is not important.

But relying on those alone is like telling people that we're delivering them cars with the brakes disabled, but they should drive defensively.

Safe computing practices are important but simply not sufficient.

The Center's dirty little secret is it is not five lab technicians in Iowa.

It is a virtual network of high-end practitioners who start with common knowledge about a particular technology -- we started first with operating systems and have moved now into market-dominant technologies in other sectors.

We have benchmarks now for a CISCO router. We're about to release one for Oracle, and for other technologies that are actually out there in use. The Center produces these benchmarks. They're available free of charge on its website.

But even more importantly, the Center produces measurement tools, non-intrusive software that actually tells you the extent to which your systems are not hardened, and you can use those on a continuing basis.

What's really even more exciting for us, to steal a British phrase, is our measure of success is not product produced.

Our measure of success is take-up rate. It's changes in behavior in the real world. And several exciting things have happened, some of which you've heard about here today.

Microsoft is beginning to produce a Center benchmark-compliant version of its newer operating systems.

Dell -- I'm going to actually take a tape of Craig Lowery's presentation this morning and send it out in lieu of any future public speaking that I do. Dell told you what they were doing. That, for us, is success.

Visa links to the Center's benchmarks in its top 12.

Our success is not in having consumers or even small businesses know about the Center but, rather, about having technology that is Center benchmark-compliant delivered to them in much the way that the questioner in this morning's session asked about how we do security so that it is transparent to the user, transparent in the sense of passive, doesn't require any active intervention.

We also have been working with the major vendors of security software.

Again, while we provide the Center's tools on our website free of charge, the typical computer user is not going to search out the Center for Internet Security but may buy tools from vendors like Symantec or Net IQ or BindView, all of which are now building the Center's benchmarks into their security suites.

Again, take-up rate is important for us, and that's a way of penetrating the market.

The Center's website does tell you far more cogently than I have what we're about and who we are, and it gives you direct access to all the products I've described. The URL is www.cisecurity -- no punctuation -- dot-org.

MS. GARRISON: Thank you very much, Frank.

Laura Berger.

MS. BERGER: Good afternoon, everyone.

The FTC has been very active in the area of security, and I'm just here to tell you about some of the latest things that we've been working on. One of those is the FTC's Safeguards Rule under Gramm-Leach-Bliley, which took effect on Friday, May 23rd. We've been talking about, as Mark MacCarthy said, fairly high-level security standards. The Safeguards Rule, for those of you who want to see it or have had a chance to look at it, is on our website at FTC.gov and accessible under our brand new privacy initiative website that's newly revamped.

It is very high-level. It applies not just to a specific Internet site or a specific type of business context but to a specific type of institution, financial institutions.

I won't get into describing exactly every kind of entity that fits under that rubric. People who have had experience dealing with Gramm-Leach-Bliley and the private notices and Privacy Rule are probably fairly familiar with it. But it's a very diverse range of businesses and entities, from very large and sophisticated entities to very small, even sole proprietorships that engage in financial activities.

It's not just about addressing Internet business but also about addressing physical storage of records and how employees handle records and what CEO's tell their IT people. It's very broad, very high-level, and it has two parts to it that I'll first just touch on very, very briefly. Then I'll talk briefly about our outreach.

The Safeguard’s Rule has a reasonableness standard for what the overall security of a financial institution has to accomplish. That standard also embodies required elements, and I won't go over all of those here, because there are five of them, and I think that would exceed the five-minute time limit if I did.

But they're high-level. For example, one of the elements is assessing risks to the security of customer information.

It's up to companies to really unpack that and figure out what they need to do to assess the risks that face their organization and the customer information they're maintaining.

What are we doing to help businesses address this new challenge? A lot right now. We're doing a lot of outreach to try to alert businesses that may not be aware of the new requirements and the way that they apply to their business.

One of the things we're doing that you can pass along to people is I will be conducting, along with another staff attorney, Ellen Finn, on June 9th and June 23rd, one-hour training sessions.

There will be dial-in instructions for participation in those training sessions posted on the FTC's website at least the day before the training sessions, and people can also come here to conference room A in this building on those two days, according to the times posted on the website.

That's our most public outreach, but we're also just handling a lot of industry queries and working with a lot of industry groups to help them apply the standard to their particular industry and their types of circumstances.

The standard which I mentioned -- referred to as a reasonableness standard -- specifies that what's going to be reasonable will vary according to the size and complexity of the business, the nature and scope of its activities, and the sensitivity of information. A lot of entities have wanted to talk to us about, what do you really mean by that and how does that really work. Of course, we can't give definitive answers, but we've been working hard to talk these things through and help industries get their own analysis onto their websites and into their newsletters, and we'll continue to do that kind of work.

With that, I think I will turn this back over for general discussion.

MS. GARRISON: Thank you very much, Laura.

The frameworks or the approaches that we've just heard very briefly discussed, as you can see, are quite varied.

Some of them are mandatory, either by statutory requirement or by membership requirement. Others are voluntary.

Some are very high-level. Others are quite technical.

Frank, as you think about this, do you find any common features or core principles among these frameworks, and what role does technology play here?

MR. REEDER: On the latter question, I have a bias, but I'll save that for last.

On the former, it's actually wonderful to hear -- it may be boring for the audience -- a fair amount of harmony around this table.

What I've been hearing -- and I think this is a growing chorus -- is we're all trying to identify, through some sort of a process, what I would call consensus best practices.

This is less, I would argue, except at the very high-end, a matter of invention as it is a matter of information-sharing.

Much of what is going on relies on, to some degree, some fairly detailed technical work.

Fran made mention of the fact that they're working on the assurance side.

The third trend I see is an increasing reliance -- and this came through in other panels and in Toby's nice phrase, baked-in security -- making security more a part of the product offering.

And I think related to that -- and here, I think both TRUSTe and Visa are teaching us about the importance of branding -- ultimately the consumer and the small business, the entities that don't have the capacity to make complex technical judgements, rely on cues in the marketplace that tell them or give them reasonable assurance that a product or a service is, in fact, safe from their perspective. We're starting to see a lot of push in that direction, and ultimately that gets to the point that several of the folks on the panel made.

This ultimately has to be market-driven. But it's not going to be market-driven based on individuals looking at the technical pieces of security and privacy but, rather, some more general set of assurance backed up by some of the organizations around this table and, ultimately, the threat of enforcement from the Federal Trade Commission if they make claims that are un-substantiable. In other words, when they see a brand or a mark that says you can expect this level of assurance and this level of protection, indeed that is a valid claim.

MS. GARRISON: Larry, what core commonalities do you see from your perspective?

MR. CLINTON: I was just thinking about it. I think I see four kinds of commonalities.

The four that I see are systemic, cooperative, creative, and ongoing.

There seems to be a consensus that technology is not the answer, training is not the answer, insurance is not the answer, international cooperation -- they're all the answer. It has to be a systematized approach.

In the same sense, everybody seems to be interested in learning from each other.

Oh, that's a good idea Visa has. Nortel is going to try to apply that to its vendors.

Oh, that's a good idea AIG has for Visa or ISA, maybe we can bring this into other things.

So, there's an attempt to cooperate here which I think is indicative of what the Internet is. It began, really, as a collaborative element.

There's creativity going on, the recognition that maybe the old paradigm for regulation, if you will, that was built off the industrial revolution and, frankly, static technologies -- automobiles, for example -- which were good, but you need to have a new paradigm, because the Internet is itself a new thing.

Individuals are much more involved. It's ongoing. It's changing. So, we need to be ongoing and changing, also, and that's the last piece, is that it's ongoing.

Nobody at the table is saying okay, I got it, now we can move on to Internet 2. Nobody is saying this is what we've done.

Everybody's saying, well, this is what we're doing, and we're listening to everybody else, and we're delighted to be here and we have to constantly move forward.

So, I think those are four macro things that I'm seeing that I think are all very positive.

MS. GARRISON: That's good.

Fran, you look at this from a privacy perspective. An awful lot of this conversation is about security. As Frank and Larry and the others here see commonalities on the security side, do you see common or core privacy principles emerging?

MS. MAIER: Yes. I think almost everybody has adopted, to some degree or another, the fair information practices, and I think that that framework has been a very powerful framework under which to develop specific privacy policies and programs.

Now, there's a lot of debate. There's debate over what is adequate choice. Should it always be opt-in and opt-out, how best to monitor for some of these things, what really is notice, and there's not only the base, there's activities, like the short notice program and the P3P program and others that try to bring more of these notice things up to the forefront.

To the point that Larry made, there's a lot of, again, creativity, there's a lot of activity. I know that, for TRUSTe, we're working right now on TRUSTe license agreement 9.0. We've been around about nine years, and that really speaks to the fact that, every year, there are more things that come up, either because consumers are bringing them up or because technology has changed, or some combination.

So, for example, in 1997, I don't think we talked about web beacons or perhaps cookies, but clearly, that's been in the license agreement for a long time.

I anticipate, in this next agreement, we will talk more about security and e-mail best practices, because right now, for a lot of reasons, those two things are coming up, and I think that evolution talks about that. You can sit here and talk about what is the best practice and where it's going to go. Sometimes you have to start a little lower than maybe you'd like, but over time, you're probably going to get to the place that you really need to get to in terms of consumer protection. That whole idea of the process being ongoing and evolving is an important concept to keep in mind.

MS. GARRISON: I think that's true.

David, can you tell us or summarize what you think has been the progress in the last year in adopting these various frameworks, and do you see any new frameworks that are under development or that are emerging?

MR. FARES: Well, I will begin by expanding upon the progress that I've seen in implementing the OECD security guidelines. By the way, I forgot to mention at the outset that they are voluntary guidelines, but the OECD governments have been working to implement those guidelines. The U.S. Government and the FTC have an active work program in that regard.

The OECD will hold a workshop in November, in Oslo, to continue to raise awareness about the need for all participants to promote a culture of security.

I already mentioned what the international business community is doing to raise awareness through the efforts of the International Chamber of Commerce and the Business and Industry Advisory Committee, but the OECD guideline process has spurred other inter-governmental organizations to also begin to look at how they can start creating awareness for the need to promote a culture of security.

The U.N. General Assembly basically adopted the OECD guidelines in January 2003. The Asia Pacific Economic Cooperation also has a program to promote awareness on cyber-security, and the EU is basically creating an information-sharing mechanism.

There are also a whole host of private sector initiatives apart from the OECD guideline process. The

International Chamber of Commerce has a cyber-crime unit where it attempts to track security incidents and provide guidance to businesses and law enforcement agencies about trends.

There are the ISAC, CERT, SANS. There's a whole host of private sector organizations that are trying to create awareness and information-sharing so that people can better respond to security incidents. As we work toward implementing these frameworks, Loretta, creating awareness is one of the most important things, because there are a whole host of resources that exist. Resources will continue to be developed, but we need to create, in the mind-set of all participants, that they need to engage, that they need to be a part of the solution, and I see a lot of progress in that regard.

I think we're in the stage today where we were probably in 1998 in the privacy debate, Fran, when people just started to pay attention to privacy and really put it on the agenda for all participants, whether it is consumers exercising their choice, or whether it is businesses promoting and adopting and posting their privacy policies.

We've seen significant progress in the privacy debate with corporate policies being posted online, with organizations like TRUSTe and BBB OnLine. So, I am confident that we're going to continue to make progress, and this awareness-raising exercise is really going to be helpful, and it is going to produce success.

MS. GARRISON: Frank, from your perspective?

MR. REEDER: Well, I think there's been enormous progress, as I said, in take-up rate, but I'd like to focus on one aspect of your question. That is are new frameworks developing.

There are risks in relating cyber-developments to the physical world, but some of those comparisons are valid. I think if we look at other areas of risk or consumer safety, something very exciting has happened in the last year in the cyber-world that happened perhaps 30 years ago in the automotive world. That is, rather than viewing security or safety as a cost, as the manufacturers were telling us when they said they couldn't afford to put air bags in cars, we see companies beginning to sell safety and security as a feature, whether it's the branding of a service, like Visa is doing, the TRUSTe mark, or Dell's announcement that you can now buy a securely configured technology at a nominal additional charge. It's a vision I've had for a long time.

The Mercedes and the Volvos in the cyber-world are beginning to emerge, and that, in turn, I would argue, just as it did in other areas, will begin to drive practice. The reality is, in the physical world, very often, then regulation follows when the dominant practice becomes something that it is unreasonable to allow others to ignore, rather than using regulation as a way of driving practice.

So, I think there has been, in my view, a significant shift in the last 12 months that is very exciting and I think should dramatically accelerate the use of privacy and security technologies.

MS. GARRISON: Fran, do you see the same thing from the privacy perspective? David alluded to it a few moments ago, saying that we're now at the stage in security where we were with privacy four years ago.

MS. MAIER: You know, I think there is some good news and some not-so-good news.

In terms of online privacy, I think the adoption of privacy statements is almost ubiquitous, especially among the larger companies -- you’ll see it in probably the top 500 -- and it's almost a requirement. Everybody thinks about having a privacy statement.

However, enterprise privacy, software privacy, product-related privacy -- the fair information practice frameworks still work, but implementation of consistency in those areas plus the ability to monitor and audit and so on has not quite emerged yet. I think it will emerge, because I think, actually, the whole effort to get security under control, which is a requirement for privacy, is driving an effort within industry to take a look at their own enterprise data flows, their own enterprise security programs and so on. Once that's in place, then hopefully the question of privacy comes up.

It is interesting. I had dinner with somebody last night who was attending the Gartner security conference, which I think is going on here in D.C. this week. The conference didn't have anything on privacy, and it struck all of us -- the couple who I was talking with -- as that's not really up to date. Hopefully they'll change that, because I think the privacy question goes along with the security question.

MS. GARRISON: We've heard different terms used -- standards, frameworks, benchmarks.

Frank, you've, of course, alluded several times to the adoption of the CIS benchmarks, but can you talk briefly about benchmarks, perhaps what they are, as distinguished from frameworks or standards? Are they helpful? If so, why?

MR. REEDER: Well, the penultimate question is easy. Of course they're helpful.

We have deliberately adopted the use of the word "benchmark" because of the baggage associated with the use of the word "standards," although I was delighted to hear on a previous panel that some in the industry are increasingly welcoming standards at this point.

The benchmarks are, in fact, for the technologies for which we developed them, hardening scripts. They're essentially a set of specifications on how a piece of software or piece of technology ought to be configured so as to eliminate known vulnerabilities.

They are highly technical documents. I will confess, as I think a previous panelist did, I cannot read a CIS benchmark and make heads or tails of it except at a fairly conceptual level.

The companion piece, of course, is a piece of software that then measures the degree to which the way your software is configured matches those.

Are they of value? The simplest metric I have -- and this is an independent measure -- is that out of the box, the technology that is generally delivered to users is highly susceptible to attack, based on studies that NSA and others have done. When the technology is hardened to comply with the Center's benchmarks, for all of the known attacks that we have seen spread around the world in the last 18 months, essentially adoption of the benchmarks would render the user of the benchmark immune from those attacks.

But the simple measure of success is does it afford you protection? Absolute protection, certainly not, but for protection against the prevailing threats that we know of, we have a very high degree of assurance based on independent examinations that have been done by others, not just by the Center.

MS. GARRISON: Are the benchmarks at level one that the CIS has available -- are they something that just the ordinary consumer can actually do, or do they really require a lot more technical expertise to install?

MR. REEDER: I think an individual who fancies him or herself as an expert user could certainly adopt them, but I think we encourage folks to use other products that do that.

That's one of the difficulties that we are encountering in getting adoption at the consumer level, and that's why we're placing so much emphasis and we're so delighted to see products being delivered that are already configured. Certainly, the typical system administrator, even if he or she is just a part-time systems administrator in a small enterprise, can implement them.

MS. GARRISON: Okay.

MR. REEDER: But whether our aging parents or uncles and aunts could, I doubt that they would.

MS. GARRISON: I was thinking more of someone who's technically challenged like me.

MR. REEDER: We'll send someone over to help you.

MS. GARRISON: Thank you.

Larry, I'd like to move to a discussion about barriers to businesses in adopting these frameworks. Can you begin the discussion?

MR. CLINTON: Yes.

I think we've all said there's a lot of progress being made, and that's great. That's a good news, bad news situation.

A lot of people say, oh, well, there's a lot of progress being made, it's not so much front page now, well let's move on to other things. That's a problem. Success can sometimes breed over-confidence, and we really have to watch out for that.

A second major problem is that, despite the creativity we have spoken about previously, a lot of corporations still view security as a cost center, not an opportunity. There are some exceptions out there, and they should be highlighted, but still, the typical investment in cyber-security is probably not what it should be, particularly the ongoing operation of things.

We've already discussed how important that is. It is something that is a problem.

People are putting in security systems, but they are not checking up on them, not updating them, not updating their training, not enforcing the procedures that they have.

There are also some market-based problems with some competitiveness, notwithstanding a lot of cooperation we're seeing.

There are a number of people who are saying that the information sharing that we believe is critical is being impeded because there's a resistance to communicating with your competitor about the problems that you have. A lot of the structures that we have are, frankly, built on the former economic model.

We started building ISACS following PDD63. We said okay, let's put all the technology guys together and all the financial services guys together. Financial service has been one of the most successful of these, but still, we've got everybody in the old silos that now we all kind of dismiss as archaic, but those are still the structures that we're working with. We think we probably need some new structures that are across industry, international, more cooperative, and I think we can still do a lot of work developing incentives.

We at the Internet Security Alliance, supported the National Strategy to Secure Cyberspace, but I don't think that the plan is perfect.

I don't think it speaks adequately to how we're going to have private sector incentives. I don't think it speaks adequately to how we're going to create good data upon which we can build an awful lot of cost-benefit models, et cetera, and these are the things that industry is going to look at.

So, I think we've got a ton of work still in front of us. We've got a number of barriers -- cultural, economic, and structural -- that need still to be broken down, but I don't want to diminish the work that's being done.

MS. GARRISON: What about the issue of corporate support?

I know that we've read some general reports about investments by corporations in their IT programs, and of the IT funds, actually it's a fairly small percentage that, on average, goes to security itself. Is that a pervasive problem?

MR. CLINTON: Well, the first principle that we have in our five principles is investing more in security. So, we think that it's certainly a problem.

One of the problems with it, which I just alluded to, perhaps not as cleanly as I should have, is that the data for what counts as security investment is pretty loose. Are we counting training in that, or is it just IT technologies, is it software, et cetera? So, it's kind of hard to really tell, even in some of the better studies, what the measurement is.

I think we need some better models, starting at the academic level, for that. But to get to your point, yes, investment is still a problem. IT investment is a problem now, and we still see that in the IT sector of the economy, and the security portion of the IT portion is a problem.

Another problem is the degree of commitment that senior management has to security -- boards of directors, CEO's, and the like.

A lot of this still resides with the CIO, not the CEO and not even the chief security officer. It's the chief information officer.

I think we have to broaden the perspective of security so that security becomes part of the operation of the corporation just the same way payroll is an operation of the corporation, management is an operation, human resources.

These are things that everybody in the organization needs to be focused on. That's our first best practice, and the first is geared to getting to senior management.

I don't think we have crossed that barrier yet. I think there are a lot of people interested. We're working with Technet on that. They're going to have a big program coming out.

There are a lot of people working on this, but that's not to say we're there yet.

MS. GARRISON: David, do you see any barriers from your perspective?

MR. FARES: Yes. I'll just expand a little bit on what Larry said, and then I will move to a different focus. But, as I said, there's been a lot of work on awareness raising. That work on awareness raising is beginning to create an understanding within the business community that security is a business enabler and not a business cost. As we move toward that as a broader understanding within the business community, where I think we're making significant progress, I think one of the major barriers will come down.

We've been spending a lot of time talking about IT expenditures, but IT expenditures is only one small element of a security policy, as many others have discussed. Training. Security is a process, and we need to make sure that all participants understand that they have to not just attempt to adopt a quick fix, but they need to implement a security policy that includes reassessment, that includes training, that's ongoing and continuous. Finally, I've alluded to it several times, but I think that many other participants feel as though security is simply a business issue.

It's not just a business issue. Everyone has to work to enhance security, whether it is a consumer, government, a network operator. Everyone has to work as an awareness raising organization.

I think there needs to just be a broader understanding, consistent with the OECD guidelines, that everyone has a role to play, and it's not just one participant's responsibility. Once we're successful in that, I think we will also overcome a lot of the barriers.

MS. GARRISON: Laura, you work with a whole industry that, in fact, is under a regulatory regime to implement security measures. What is your experience as to the barriers that may be impeding the adoption of frameworks in this area?

MS. LUNDIN: Well, I have a couple of comments.

First of all, I echo a lot of what has been said amongst the panelists about the necessary change in culture needed on behalf of the product manufacturers and the service providers to actually build in that security and the need to value security as much as the business functionality that comes in a product or the processing capabilities on behalf of a service provider.

So, I think the need to value security is still a primary impediment to adoption of some of these frameworks.

On the other hand, it's also very difficult, I guess taking the stance from an organization that tries to create these frameworks, to strike a balance. You try and be high-level enough so that it is a flexible framework. You can't be too prescriptive within the context of risk management.

Various situations are going to require different types and levels of risk management. So, you have to account for that, and you have to maintain that flexibility within your frameworks.

On the other hand, if you get to too high a level, people don't have that understanding, and there's certainly a learning curve.

A lot of the regulatory regime that's come down on behalf of the financial regulators was very broad-brush. It's taken several rounds of examinations for these organizations to really figure out the intent and the level to which the regulations come down and then, in turn, how they pass that along to their service providers or their product manufacturers.

So, again, trying to strike that balance is a real challenge.

MS. GARRISON: Frank, what about small businesses? Are there special challenges here?

MR. REEDER: Absolutely. I think one needs to make an important distinction between large enterprises and small enterprises, which in many ways behave more like individual consumers, at least in the information technology marketplace, where it's not reasonable to expect that there is technical critical mass within the organization.

It's probably the youngest person in the organization who gets you out of trouble when something goes wrong, but there again, the small business is more reliant on buying safer products.

Certainly, education can help with respect to management practices, but there's one other actor we haven't talked about in this conversation, and that would be the service provider, the VPN provider or ISP. There, again, we need to look to that sector to build more security and privacy technology into the offerings that they provide, simply because it's not reasonable to expect individual consumers or small businesses, apart from the cost question, simply to spend the energy. It's not a question of being smart enough but of being able to spend the energy to make the technical judgements that they have to make.

MS. GARRISON: Laura Berger, I know it's a little early to do an evaluation, because the Safeguards Rule just went into effect, but are there special barriers or issues that you've become aware of in this short period of time?

MS. BERGER: So far, some of the panelists have addressed these. My evidence is very impressionistic, but it is a cultural issue, and change is kind of slow.

We've had meetings with lots of industry representatives, and without picking on anyone by identifying them, I've met with large groups where their message has been we just don't think of ourselves this way, and I think that it's going to take time before people start to think of themselves this way.

And to echo what Laura Lundin was saying, as well, the standards that the agencies put forward are fairly general. I think it takes time to translate those into specific practices and to figure out what works over time. Building on what Frank was saying as to service providers, there is a requirement in the Safeguards Rule -- and this is just one example of one of the many changes that's got to come about and really get streamlined through practice.

There's a requirement that financial institutions oversee their service providers, including by entering into contracts with them. At this point, I think one of the barriers that I'm seeing is there's not yet a streamlined process for how that's supposed to happen. We've been concerned about this all along and really tried to anticipate, but we have, for example, small businesses saying, well, what kind of agreement should I enter into with my data processor? Some of this eventually is going to have to come from the service providers.

They're going to have to start off with built-in security guarantees to their financial institutions so that these things won't be negotiated in an inefficient way.

I already said that we're trying to get at this through education and through outreach to the industry. We're also working to educate consumers and raise awareness and demand to help bring about the cultural change that will make businesses see it in their interest to provide security.

One of the nice publications available on the table -- and I can honestly say one of the few with color illustrations that's available to you, is our Internet security initiative publication featuring Dewey the turtle. It's our big consumer ed piece talking about what consumers need to do to stay safe online. I point smaller businesses to it at times to say this is what's appropriate for you, because, as Frank was saying, you're a lot more like an individual consumer. The rule is adaptable to your situation, and you can look at these kinds of measures to address your needs.

So, I'm seeing a lot of need to synthesize these broad standards into streamlined practices that businesses can keep a handle on.

MS. GARRISON: So, the common consensus here is that we need to figure out ways to translate these principles into practices, and we've already started talking about some incentives.

I know, Larry, you've already mentioned some. Do you want to quickly summarize some of the incentives that you see in the marketplace or elsewhere to adopt these frameworks?

MR. CLINTON: Well, I think we've already probably hit on most of them.

We try to lower business costs.

So, if you'll adopt best practices, you'll get less insurance cost.

If you do training, we'll get you discounts.

We're very supportive of the Visa program, and we try to encourage that sort of thing with our other member companies.

I think one of the things that’s been alluded to here is that those corporations with -- I use this term in quotes, an advisory -- "market power" can use that ability to improve security in their own enlightened self-interest.

While I'm sure that, in Visa's case, Nortel's case, and a bunch of other cases, it was done out of an awareness of security and the public good, I'm sure there was also a recognition that an insecure network is economically threatening to the corporation.

I think that a whole lot of corporations still need to embrace that and insist that, if you are going to be our vendor, if you are going to be our supplier, if you are going to be our customer, we need for you to adopt this system of security, because the Internet is an interwoven network of networks, as everybody in this room knows, and a threat to one is a threat to all.

I think there's a lot more creativity that we think can happen, but as I say, we really need to work on a new paradigm.

The old regulatory paradigm probably doesn't fit this one.

We need to be a little more creative. I think there's a lot of creative ideas out there, but I'm sure we haven't exhausted the market on them.

MS. GARRISON: This, I think, plays into Mark and what you've been doing in your CISP principles, because from what I have heard it sounds as though branding and consumer confidence were drivers in adoption here. Do you want to speak a little bit about that?

MR. MacCARTHY: I think the major points have already been made.

You know, security is a large topic that crosses a lot of different industries. So, I can only really speak about the incentives that Visa might have had for doing what it did, and it's only in the area of keeping card-holder information safe and secure. But there may be ways in which you could generalize our experience to other companies, as well.

When we looked at the Internet several years ago, we saw some concerns about the security of online shopping.

We saw security as a major threat to the development to that channel of commerce, and we saw it as a potential brand problem for Visa, being associated with an insecure method of payment. For all those reasons, we decided to step forward and make our program not just a set of “we hope you do this kind of practices” but requirements for actually taking a Visa card.

At the time that this was first being introduced, there were a large number of Internet hacking incidents, there was large publicity about them, and so, we got a pretty receptive audience initially, because people realized that what we were putting forward were ways in which they could then turn around and protect themselves against a business threatening possibility.

The biggest troubles we ran into were when we insisted on audits, when it wasn't just us saying we want you to prove that you're doing the right sort of thing not to Visa but to independent outside security assessors.

A lot of companies would say, well, we do it ourselves, we already know how to do this, why do we have to go out and prove it with an external assessment? We had a lot of discussions in that area, and I think we've gotten over that hump.

A lot of people realize that, in this circumstance, you can't take people's words for it when they're repositories of very, very large amounts of card-holder information.

So, that's the way our program has developed so far.

MS. GARRISON: Fran, we've heard Frank speak earlier about the shift in thinking from the product developers who are now seeing security as a feature rather than a cost.

Do you have any experience on return on investment, because that clearly seems to be an important driver here for corporations.

MS. MAIER: We're always looking for ways to help a company not just talk the talk but to walk the walk and really have the real commitment to privacy. What we have found, while we might be very successful with the chief privacy officer or the risk manager or the general counsel, legal counsel, and they believe that having sound privacy practices and the seal program makes sense, it's the marketing people and the people who are driving the revenue that we want to try and convince.

And we're undergoing a lot of different studies to try and figure out the pay-back for privacy or for the seal program. I'll talk about one I think you'll be hearing more about in the future, about a little company called Big Dates.

They're not a dating service. They do anniversary-related kinds of things -- birthday party, reminder service -- and they sent out, randomly, 80,000 e-mails. 50 percent of them had the TRUSTe seal at the bottom saying we protect your privacy. They had the seal linked to the privacy statement.

Well, the company saw a 40-percent increase in the join rate and the click-through rate, and that's pretty remarkable.

Now, that's not a well-known brand, but I think it shows that the consumer recognizes TRUSTe. Overall, we're talking to a number of companies who are joining our program to do testing. What's important about that is that it's going to put even more emphasis on having the right programs and the right enforcement and the right strength behind the seal, because if it means that much, then it really has to deliver both for the consumer as well as for the organization.

MS. GARRISON: Mark, you mentioned earlier about accountability. That also seems to be a common theme that's popping up from various panelists.

Can you talk more specifically about how companies in the Visa system are held accountable for complying with the CISP principles?

MR. MacCARTHY: It's indirect. Visa is an association of financial institutions. So, we have no direct relationship with Internet merchants or processors or web hosting companies.

So, the mechanism we use to make sure that these requirements move out into the marketplace is through requirements we put on the banks that work with the Internet merchants.

If there's a problem with a particular merchant where they haven't fulfilled the requirements of the CISP program, then ultimately a fine goes on to the bank that works with that particular merchant, and that merchant bank then moves that penalty on to the merchant.

Ultimately, the way of enforcing the mechanism is through continued membership in the Visa system. It's clearly possible to make sure that merchants aren't permitted to use Visa cards. We enforce that, as I say, through the system of financial institutions that are part of the Visa system.

MS. GARRISON: And have you already taken action, either fines or other types of action?

MR. MacCARTHY: We've had a major processor who did not live up to the responsibilities that it had under the system. We fined them $500,000. They're under suspension right now.

MS. GARRISON: That must have served as a wake-up call to everyone else who participates, too.

MR. MacCARTHY: It catches people attention at high levels.

MS. GARRISON: Yes, I should think so.

Frank, do you have anything more to add about accountability? How do we get there?

MR. REEDER: Accountability is tough, and I guess all accountability ultimately occurs in the marketplace. I would also argue for it -- and here I'm echoing what Mark has already said -- through independent audit. We, again, also haven't talked about the audit community, but they're a part of the assurance network that ultimately goes to fundamental questions that are being addressed by things like Sarbanes-Oxley.

I would like to be mildly contrary on one small point.

MS. GARRISON: You have the privilege to do so.

MR. REEDER: Thank you. Lest this sound like a chorus.

It's probably true that we're not spending enough on security, but I think, as Larry said, quite correctly, we haven't the vaguest idea, because we don't know what we're measuring.

Starting with the fact that developing good software is essential to good security and the ability to provide the privacy assurances. I'm sure nobody is counting that in their security budget, so I simply don't know how one measures that. Probably the deltas are meaningful assuming that people are consistently measuring. At least we can see change from year to year, even if the base number is mush.

But I think it's even more important that the money we're spending, we're spending badly. Again, what you are hearing from this panel and I think the message that needs to go out is the way you start a good security program is not to hire a very expensive consultant, with apologies to the very expensive consultants who may be in this room, to do a zero based risk assessment when we already know that there is a set of baseline practices that you ought to be implementing and auditing yourself against and then looking at whether there's differential risk, whether you are unique within your industry or sector and ought to be doing something beyond the baseline.

But we've got it exactly wrong. There are a lot of people making very good money -- unfortunately, I'm not among them -- who are selling the same snake oil over and over again, rather than promoting the adoption of knowledge that is already in existence and that is available relatively inexpensively.

Most of the things we're talking about here are not expensive, and so, I would argue that the problem is not money. It may well be how it's being spent.

MS. GARRISON: On that high note, we'll open it up to questions.

Is the microphone working? It is now. Okay.

Brian.

QUESTION: Brian Treddick from Ernst & Young.

I just wanted to call to the attention of the Commission and the participants in the workshop the American Institute of Certified Public Accountants and the Canadian Institute of Chartered Accountants released yesterday another framework, enterprise privacy framework, after about a year-and-a-half of development, friends and family review period over the winter.

It's open for a three-month cycle of review -- June, July, August. We’re hoping to get comments from everyone to make it stand out as what we'd consider in the industry as established criteria.

The goal is to allow a company to assess and align its practices around the handling of personal information or allow a public accountant, a CPA, an auditing firm, to come in and audit some set of systems and processes around it.

So, it's available for download, and if you have any questions, I'll be around for the rest of the afternoon. I can answer those then.

MS. GARRISON: Thank you very much, Brian.

Yes. Go ahead and state your name, please.

QUESTION: Thanks. My name is Allen Wilcox. I work for the Vanguard Group.

The question I have for you -- despite my profession's dominant certification and professional organization, it's not just information systems security, it's information security, whether it's in a Rolodex, a baggie, my head, or a computer.

How are any of these frameworks addressing non-technical information security rather than just the places where things are stored and patched and systems are maintained?

What about the actual information -- because systems are just capital assets. Is the information itself being addressed within these frameworks?

MS. GARRISON: Larry?

MR. CLINTON: We agree with what you say. We have copies of our best practices, and we agree completely with that sense.

The first thing that you'll see in our best practices is that you need to have a policy for information security, not just Internet security, and in fact, it includes physical security. Although, frankly, a lot of the same procedures still apply -- you need to have a policy, you need to enforce the policy, you need to assess the policy on an ongoing basis, you need evaluation -- these are all spelled out in our best practices comment. At this very moment I'm aggressively trying to get people to embrace these.

I completely agree with Frank's comment that there's a lot of stuff that's pretty good that's already out there. What we'd like to see is us moving away from, hey, let's write something new. I'm sure there's lots of new stuff that needs to be written, but let's implement what we've already got, and let's then evaluate that systematically. Then let's rewrite it and move on. I'm sure that's necessary.

MS. GARRISON: Laura, did you want to add anything to that?

MS. BERGER: Sure.

In my opening remarks, I mentioned that the context of our rule takes into account all aspects of how an organization deals with information and not just transactions on the Internet, and that's really embedded in the requirements of our rule. Just to give one example.

In assessing its risks, a company has to take into account all areas of its operation, and we spelled out three particularly essential ones that are required. One of those is employee management and training, and that's been one of my favorite ones to talk to people about when they call with really difficult questions about how to implement some online protection and they're just really grappling with it.

I just say, well, have you trained your employees yet, and typically, the answer is, well, no, but we haven't really drawn up our employee training plan yet. So, we tried to build that into our rule.

MS. GARRISON: Frank?

MR. REEDER: Yes.

If I may set aside my Center for Internet Security role for the moment and step back into other personas, the whole privacy debate as we know it probably was prompted by a book most of us read for different reasons by George Orwell and the revelations in the '60s and '70s that technology was being used in ways that we didn't anticipate. But if you look at the laws and principles underlying it, there's nothing about technology in the Code of Fair Information Practices or, for that matter, in the Federal Privacy Act of 1974.

It's about information practices, and your question is exactly right. All of the prescriptions that we've talked about have nothing to do with the manner in which the information is stored and processed and everything to do with the processes and content.

Your question is a very healthy reminder that a robust privacy program and an assurance program that supports that cannot stop at the boundaries of the technology system.

MS. GARRISON: With that, we're concluding this panel.

Please be back at 3:15 for panel four, and I would like to thank very much each and every panelist here this afternoon for their contribution to this discussion.

Thank you.

(Applause.)

(A brief recess was taken.)

PANEL 4: Designing Technologies to Protect Consumer Information

MR. SILVER: Welcome back, everyone, to this session, which is not only the final panel of today but the final panel of this pair of workshops which began in May.

This panel will consider how to design technologies to protect consumer information.

Are the microphones working? All right.

And to that end, we've gathered an impressive group of engineers and policy experts.

First, we have Edward Felten from Princeton

University, Alan Paller from The SANS Institute, Richard Purcell from the Corporate Privacy Group. Howard Schmidt is with eBay. Toby Levin will be helping me moderate. Ari Schwartz is back for more from the Center for Democracy and Technology.

Tony Stanco is with George Washington University. We've got Vic Winkler from Sun Microsystems, Kathy Bohrer from IBM Research, and Peter Neumann from SRI International.

I will begin with Peter by asking him to define the problem that we're facing in this area of technologies and designing them to better protect consumer information.

MR. NEUMANN: Thank you.

I would begin by saying that I am a technologist in my 50th year in this field, so I've been around a long time. I'm also an anti-technologist in the sense that I am very concerned about the misuses of technology. I will draw on both facets of my life in what I have to say very briefly.

I go back to Multitex, which was probably the most secure commercially available system ever produced, from 1965 to a couple of years ago, when it was finally decommissioned. In 1972, we did the first very reliable fly-by-wire system for NASA.

So I've been heavily involved in really high-tech technology.

On the other hand, I think we seriously tend to over-endow technological solutions, and I'd like to follow up a little bit on that.

If you think about the repeated statement about defense-in-depth, what we really have is weakness in depth, and I'd like to point out that we have flawed requirements to begin with.

We have flawed evaluation procedures.

We have flawed systems, including legacy systems and systems that require hundreds of patches.

We have flawed administrative procedures.

We have a tremendous burden that we're putting on systems administrators for the very simple reason that those systems are so difficult to maintain.

In fact, the U.S. Government is now widely out-sourcing system administration, as well as software re-deployment.

If you remember the Y2K problem for the air traffic control system, the entire upgrading of the system was out-sourced to the People's Republic of China, unbeknownst to the technical people at the FAA. This is a very strange example of out-sourcing.

We have flawed procurement processes where the government folks, in particular, are severely constrained by the procurement processes.

We have the risks of un-trusted outsiders and trusted insiders who are not trustworthy because of the fact that the systems themselves are not adequately secure, and we have an enormous lack of accountability.

We talk here about privacy problems and security problems.

The identity theft problem is one that typically comes to mind, where the average individual doesn't think that they have anything to hide, and yet they are vulnerable to identity theft.

But I would like to give you an example of one prototypical or paradigmatic example of a system that requires privacy, security, integrity, and accountability, and a lot of other things -- prevention of denial of service and so on -- and that is the electronic voting problem.

In all of the electronic voting systems produced by the major vendors who are, in fact, providing something like 70 percent of all of the voting machines in the country, there is absolutely zero accountability that your vote goes in correctly and that it's counted correctly.

This is an appalling situation. The fact that we're trying to make your votes private and provide some sort of assurance to you that nobody can figure out how you voted has resulted in systems in which the integrity and accountability and security issues have been essentially completely ignored.

The Federal Election Commission standards are lame. They're inadequate. They're fundamentally flawed. The evaluation procedures are almost non-existent. There are certification procedures, but they're based on flawed standards in the first place. The result is that we have systems that effectively have no assurance that they're going to do the right thing.

So, I think the confluence of security and privacy and accountability and availability and survivable systems that don't fall apart all by themselves without attacks suggests that there is a problem where we have, in a fundamental way, fallen short of what is needed.

Counter to the very rosy glasses picture that we heard in the previous panel, I wanted to throw out this contrary view that there are some systems that are fundamentally flawed. If we look at, say, the critical infrastructure protection problem, where we see that all of the critical infrastructures are dependent on telecommunications, on computers, on power, and in many cases on the Internet, which may surprise some of you, and the fact that all of this is completely interrelated, and the fact this was pointed out long ago by the Marsh Commission in '97, it suggests that we are not progressing as fast as we should.

Now, the standard free enterprise version is, oh, the marketplace will solve all these problems. I claim that the marketplace is not solving the problems that I have been working on for the past half-century, namely very survivable, very secure, very reliable systems.

They're certainly good at producing lots of features and whiz-bang Power Point systems and things of that nature, but I think from the point of view of what can be done to make these systems robust, the marketplace is simply not driving it.

Now, you might say, well, gee, there's the open source world. Perhaps if we made the voting machines open source, it would solve the problems. Of course, they're all proprietary. The vendors say that if anybody could ever look at the code, it would decrease the security of the system, therefore nobody is ever going to look at the code.

I happen to have looked at the code for one of these systems for New York City over a decade ago, and my conclusion was, even if this code was perfect, here are a couple of dozen ways in which the election could be rigged using this system.

So, I think the fallacy there is that, gee, if only we could look at the code, it would solve the problem. It doesn't solve the problem, and there are many examples.

For those of you who are techies, you remember the Ken Thompson Trojan horse that gets installed in the system with absolutely no evidence of anything in the source code. It happens to be an object code modification to a compiler so that the next time your source code is compiled, this Trojan horse is planted in your system.

The bottom line here is that we're dealing with end-to-end holistic problems, whether it's privacy or security or reliability or safety or whatever, and the weak link phenomenon is really one in which we are dealing with weakness in depth.

Frank mentioned snake oil in the previous session. We have a lot of smoke and mirrors, placebos, bait and switch, shell games, and certainly in the electronic voting machine case, the vendors are all saying, look, we test these things. We have a pre-test before the election and a post-test, and that proves that the system must be doing the right thing.

For those of you who are computer scientists, you realize that that's sheer and utter nonsense. Yet, the claim is made that, because these systems are certified, they must be secure.

Now, it turns out that for one of the main vendors -- after the system is certified, the way they install the ballot face for a particular election is they change the code, after it's been certified, and they put this new software into each of the precincts' systems, which is different for each ballot face in each precinct, and they say, oh, but it's been certified. Okay?

I suggest again that we have a weak link phenomenon which has too many weak links in it.

So, very briefly, given the holistic nature of the problem and the tendency that we have to grossly oversimplify problems, I think the issues that we have to deal with suggest that we really need to look at technology as a holistic problem.

If somebody tells you that they have certification procedures or they have best principles or whatever it is, this is one piece of the puzzle, and all of that is good, it's useful, it's helpful, if you remember that it's only one piece of the puzzle. The real problem that we're dealing with is that in most of the critical applications that I happen to deal with all the time with safety, reliability, security, and so on, ultra-critical systems, any weak link is enough to demolish the integrity of the system. Yet, if we have a system which is nothing but weak links, we have essentially no assurance.

So, I offer you as a paradigmatic example of this whole thing this election system, the all-electronic voting machine, with essentially no assurance that your vote goes in correctly. I suggest that you try to apply all of the wonderful techniques that we heard about in the previous session and try to seriously apply them to that problem.

Open source would help a little, maybe, but it's competitive. Everybody is writing their own systems.

At the moment, there is no way of telling when something has gone wrong whether it was an accident or whether it was fraud, because there is no accountability.

It is impossible to do a recount, because the bits are already there. If you do a recount, you get exactly the same result, even if it was completely flawed.

This is the bottom line that we're dealing with, and I can go on for another five minutes, but I think I'd better stop at that point.

MR. SILVER: Thanks very much.

Howard Schmidt, how do you view this problem?

MR. SCHMIDT: Well, I'll start with the piece that I agree totally with what Peter said, and that's the fact that this is not just a technology issue. We've said for a long time it's the other PPT -- the people the process, and the technology.

As Peter related to, some of the early operating systems were very secure. We've seen some A1 systems that were secure.

No one bought them, because they were that difficult to use.

So, consequently, there was always that sort balance point that people were looking for. But oftentimes, as I look around and I see intrusions in the systems, I see flaws in systems, I see the way things occur, and sometimes it's about the coding itself. The errors that are made in the code, which we've been dealing with since -- 1976 is the first one I'm aware of, in which an intrusion took place due to a bad code in a proprietary operating system. But we also see, in many cases, configuration mistakes, and that goes to Peter's point that I'm in agreement with that these things are way too hard. They're designed not to be simple anymore.

And thirdly, the other piece that we see are errors that occur not just because of configuration, but because of an inability to maintain a system. It's interesting, because I try to put things in the analog world and compare to what we've seen over the evolution of automobiles.

In the very beginning, those that owned cars were people who could fix them themselves. I think back into the early days of the PC revolution in the early '80s. Those of us who could were doing it because we could fix them ourselves. Since then, like cars, we've made PCs easy to use. We can all do things with them, but we can't fix them.

We can't do our own brakes anymore. We can't, in many cases, repair our own computer systems. So, consequently, we can do more with our cars and computers. We can go faster in a car, we can do a lot more with a PC, but it's more complex to fix them.

Now, I do want to switch for just a moment and discuss something that I am not in full agreement with Peter on, and that's about the role that the market plays in this.

I think, significantly, having been there from the early days in the Marsh Commission to the private sector, back to the government and back to the private sector, I see a tremendous desire, true, genuine desire by industry to do better, to the extent that people are spending millions of dollars of research and development from all of our major companies. Some of them sitting here at the table with us, some of them in the audience today. They are putting real dollars behind the problem, but the problem is it's not going to happen overnight.

We have built a system that has some flaws built into it. We're not going to be able to repair it overnight. We're not going to be able to, as I mentioned once before, even if we were to turn around tomorrow morning and hand everybody a CD with a secure everything, from a web server to an operating system to a word processor. If we were to turn around and do that tomorrow, we would still take three to five years before everybody would upgrade, because everybody has to migrate and remediate and do all these other things.

I'm not in concurrence with the view that market forces aren't working.

In closing, I just want to, once again, look at the broader perspective that Peter brought up about all the different ways one can do things. Once again, you're looking at this in the analog perspective.

There are ways to break into a home. You can kick the door down, smash a window, mess with the garage door opener and get the door to open, wait till somebody takes their car to a automobile place, make a pass key for the home.

There are a lot of ways to do this in the physical world, and we've not solved those problems yet. They're a lot more tangible and a lot easier to solve, I would think, than in the electronic world, where many of the folks that are using the things don't even understand what's under the hood.

So, consequently, it goes into an area where we need to continue to work, because they are working in the private sector -- to make the technology self-healing, self-repairing, and self-configuring, to where security and privacy are, indeed, part of what we're doing.

Thanks.

MR. SILVER: Thanks very much.

Kathy Bohrer -- I know you have some slides, as well, if you'd like to go to the podium.

MS. BOHRER: Can you hear me? Okay.

So what I was going to do is just give a little taxonomy of privacy research areas, to give a broad view of technology that we look at when we look at privacy.

I'm from IBM Watson Research. I work with research teams, also, in Zurich and Almaden and Tokyo, plus we have a privacy institute that's made up of external members from academia, from governments, and from companies that helps guide our research and set our agenda each year.

Anyway, this is just the little chart we use. It's got several areas in it.

The first one is privacy enabled services and applications.

That's where we would look at very high-level privacy problems like new services or new applications, new ways of doing things that would just give people improved privacy over what they have today. So, it's at the top of the stack.

It's a long way from the physical security that people have been talking about, at the opposite end of the spectrum, just how could you do things totally differently that would not intrude on people's privacy as much?

Federal identity management is one of those things. We heard about that in the first panel. Anonymous payments is something David Chaum has been working on for some time.

We have done a little research in something you might call privacy rating services, which is, you know, how do you help users understand privacy policies and be able to actually decide whether they would consent or not, opt in or not, to something that's presented to them on the web?

Well, one way that some researchers experimented with was you start accumulating a body of evidence of what people have agreed to.

You start tracking what policies people consented to, and didn't consent to. Then you start providing that information in summarized form, both to enterprises and to individuals, with comparison, so they can see, well, is what this company asking for in terms of the policy they're promising and the consent they want -- how does that compare to what everyone else has agreed to or what other companies ask for that are trying to provide the same service? That's one way to start getting a handle on what the social conscience is around what should be acceptable and permissible and what shouldn't.

This next area of privacy management is some of the things we've heard already in other panels. It's the more concrete stuff about helping your enterprise classify their data.

Of course, unless you know what personal information you keep in your systems, or outside your systems, for that matter, as somebody brought up in the last panel, in Rolodexes or whatever, it's hard to figure out what privacy policies you should apply to it.

Possible extensions to databases to push privacy control down to the same level that we push security access controls on data.

Negotiation of policies. P3P. When they first started out, they tried to do more with that standard than what it has actually ended up to be. I think there will be more as time goes on, but the idea is that it shouldn't be so one-sided.

Companies shouldn't just say what the policy is and then users have maybe some opt-in, opt-out choices. Otherwise, their only other choice is to find a different company to do business with. Perhaps there should be a little more negotiation.

But of course, one of the problems with that is most consumers would be overwhelmed if you really gave them a lot of choices to set the policy. So, we also study user models and user interfaces and how to try to get some of the complexity out of helping users know what rules to set.

That turns out to be particularly important in collaborative applications. Calendaring systems is an example. Location services through your PDA is an example.

Those are cases where it would make sense and most users want to say who they're willing to have locate them on their PDA or in their car, who can actually look at their calendaring system, and all these kinds of things. To a small extent today, some of those systems allow users to make those choices. But if you imagine extending that to the richness of a privacy policy over all of your personal data and what companies can exchange the data with each other and use it for what purpose, it can be overwhelming.

Data minimization. I actually think this is a really interesting area, because it's totally different from the idea that, well, what we're going to do is we're going to set privacy policies, enforce privacy policies, help people understand privacy. This is saying, well, let's just get away from using personally identifiable information. Let's try to redo our business processes wherever possible so that we don't need personally identifiable information.

Let's randomize it for purposes of analysis, saying we're just trying to analyze data to determine our market direction in some products or something.

We may have no need, really, to know whose data that is. There are algorithms to randomize large amounts of data like that, so, in fact, it's impossible to go back and figure out whose data it was. Yet, the accuracy of your data mining results is still good enough for the results that you need.

The anonymization work, anonymous transactions, and cash, and things like that, I think are also an example of this, where you just get away from having the personal information, and therefore, you get away from the problem.

Privacy is protected by either anonymizing information or summarizing it or randomizing it or some approach like that.

There is, as many people have said, privacy at what I consider the hard level that relies on security.

If you don't have security, then you can't have true privacy.

There's also research in extending security mechanisms to handle privacy concerns, and one of the ones I've personally worked on is access control.

You can think of enforcing privacy policies as just another kind of security -- access control. It's just that it's much more fine-grained, because you might want to have a different rule for how people use your business phone number from how they use your home phone number. So, that's a very detailed thing.

Plus, I might be willing to have my phone number used in a different way than Peter might have wanted his phone numbers to be used. So, it just gets to be very much more fine-grained in most security access controls, which would generally be on the type of data, phone numbers, and the same rule would apply to everyone's phone number.

Different people might have access to phone numbers and other people might have no access to phone numbers, but it's unlikely you'd have security policies that said, well, you have access to Kathy's phone number but not Peter's.

MR. NEUMANN: Unless you're unlisted.

MS. BOHRER: Yes. So, that's an example we actually do have today, probably one of the very few examples we actually do have today.

Then the other part of privacy where you need to extend access control is, of course, with purpose, and we heard that a lot.

Since this is about misuse of data, you want to know what the data is going to be used for. By that, we don't mean just whether you're going to read it, write it, or delete it.

We mean what you're going to do with it after we give it to you. Are you going to give it to someone else? Are you going to use it in order to fulfill the order that I asked you to fulfill? Are you going to use it to sell it to somebody else because they want to send me marketing material I don't want? Things like that.

Cryptographic protocols are another area of security technology, but it's also very important to privacy when you start talking about trying to anonymize things or de-personalize things.

Violation detection -- I think we've talked about that.

Steve Adler presented one of IBM's products that helps you enforce privacy policies in real time or to create an audit log where you could go back and analyze it after the fact.

Finally, I don't know how many people are actually doing work in this, and maybe this is getting at some of what Peter said -- you could do all this technology with the kind of software and hardware controls that I would probably come up with, because I'm really an engineer, not a researcher, but some scientists would say, well, yeah, but I could find a lot of holes in that unless I do a formal certification and verification, perhaps formal languages would help. So, there are things we can do to make the solutions we come up with much more rigorous.

That's what I had.

MR. SILVER: Thanks very much.

Ari Schwartz, are the technologies we've described so far up to the task? What else is needed?

MR. SCHWARTZ: Well, I think everyone, so far, Howard and Peter, in particular, talked about the fact that technology alone is not enough to do this. Howard said people, procedures, and technology, PPT. Nuala Kelly, earlier today, said P4P -- people, procedures, policy, and practices, adding the policies and practices side. I do think that that does get us a little bit closer to what is needed, a full framework there.

Good policies are, in some ways, more important than the technology, because they're what the technology gets framed around.

So, the policies really do have to be in place, and procedures have to be in place before the technologies can really kick in and work.

And I just want to give one quick example of what I mean by this, so that we can get to the point where the technology and the market forces really do kick in and improve privacy and security. That's in the ID management area.

You can have the new ID management technologies, but they have to be based on something, and right now, our ID management structure out there is broken.

If you look at the breeder documents, the documents that create other documents -- that is, driver licenses, Social Security numbers -- they are documents that, right now, are fundamentally corrupt in some way or another. The fact that we have to base other systems on these old systems that are broken causes problems down the road. No matter how good a technology we create for identity management, if it's based on this quick-sand model, it's going to be flawed.

Insider fraud remains a problem because of those other issues involved in ID management, and the security is still weak in ID management.

Now, technology can help solve especially those two latter problems to some degree, but they can't answer all the problems.

So, it goes back to what we've been saying ever since the FTC's been looking into the privacy issue in the first place.

Technology does play a role, a very significant role, but it's got to be teamed along with best practices, self-action by industry, including education and training, and lastly, baseline legislation that really does protect individuals.

Without all three working together, the technologies will not do enough to secure privacy or security, for that matter.

MR. SILVER: Richard Purcell, do you care to weigh in here?

MR. PURCELL: Yes. I'll represent the people today on this panel.

Oftentimes technology is developed to function in ways that it does just because somebody figured out that it could do it.

My example of that would be peer-to-peer file sharing, particularly for music swapping. You know it could happen, right?

People figured out you could do it. You could listen to everybody else's music. Everybody else could listen to your music. Great.

Now, cool technology is the kind of technology that fills a purpose, but I've never driven a Porsche. So, would it be okay if somebody invented a technology that allowed me to drive somebody else's Porsche? Well, no. That's using somebody else's property without necessarily their permission. So, why is it okay to do music swapping?

We often overlook the fact that people have a reasonable sense of what's right and what's wrong, and technology simply overrides that, just because it can override that. It's so easy to do.

So many of our privacy and security violations aren't really because of flawed security practices. The technology actually works exactly the way it was written. It's not broken. It works that way.

And it works that way not because the security around it is flawed. It's because the individual said, geez, you know, I can either take a shortcut, which is a completely human kind of approach to problem-solving, or it's because they said wow, cool, I think it could do this, but I'm going to be very obscure about putting this in, because it's just because I can do this. Nobody is going to know about it. I'm the only one who is going to know. This is the old security by obscurity model that says, essentially, there's a back door into this thing but nobody knows about it but me, so that's cool, that's okay.

Well, there are a few vulnerabilities now that have exploited those back doors, and now we know that that's not okay to do any longer.

I've had personal experience that was rather dramatic and psychically damaging, when a grid was placed on the electronic registration process in Microsoft products, and it was placed there because it could be.

A developer, without documenting it, without saying anything about it to anybody -- it wasn't on the spec, believe me -- said, hey, you know, we could do this, and maybe it will be useful someday.

Well, of course it's useful some day. It's useful to spy on people.

So, the point is I'm here to represent the people, both internally and externally, both the perpetrators, as well as the victims.

Perpetrators often just don't know better. A lot of developers that I know are not socially gifted and fully implemented human beings in a lot of ways. So, it is our job as individuals who have a policy framework, who have the ethical framework, who know what the long-term vision is -- not just can I ship this code on time, can I make it do all the whiz-bang things it's supposed to do -- but go beyond that.

Those are the people where I think the flaws are stemming from.

Those are the people who aren't providing oversight.

Have you seen the specifications for most software? I mean, really, the real specifications.

MR. NEUMANN: Typically there aren't any. Typically it's I want to make it do this.

MS. LEVIN: Richard, what about quality control processes? Is this an industry that doesn't have as much quality control as we think there is in other industries?

MR. PURCELL: Well, I'd say that the level of quality control is completely commensurate with the way that we specify what it's supposed to do. Okay.

So, I want a lock on that door. Somebody puts a lock on the door. Well, damn, I can't get through that door, because the lock only operates during working hours, and I have legitimate reasons to go through it at other hours.

Is that a quality problem? No, it's a specification problem.

So, most software works the way it's designed to work.

Software can't work against its own design, right? Is that right, Peter?

MR. NEUMANN: Pretty much.

MR. PURCELL: It pretty much can't do things that it isn't designed to do without being modified. So, if it is vulnerable, that means it's designed to be vulnerable.

Now, that might be through negligence, it might be through shortcuts, it might be through stupidity, it might be through maliciousness, who knows? But pretty much it works the way it's designed to do.

So, it's a question of planning and oversight in the first place. Quality control is certainly part of that, but it's also the specification.

We have to start thinking about this world not as a landscape.

Landscapes have trees and mountains and streams and things like that, but we essentially will sacrifice parts of that landscape, because we're only thinking of that part. But you cut the forest, it erodes the hill, it clogs the stream, and it kills the salmon. It's not a landscape. It's an ecosystem. It all works together.

So, you can't say it's okay, fine, I don't care, just shortcut this, just do that, it will be okay, because we think of those decisions as isolated decisions that only have the impact over the things that we are conscious of at the moment.

The problem is it makes guys in this room, in this panel, get old really fast.

Howard's 19 years old.

(Laughter.)

MR. PURCELL: The problem is that we're not thinking long-term very often. We're not thinking very far in the future.

Howard just said, look, even if we produced technology that was perfect, it would take it a long time to deploy it.

Why is it that privacy and security have rather suddenly, in social terms, in time, become a screaming issue. Why can't technology, which we all think of as incredibly rapid, solve this issue very fast?

Well, it's because technology isn't that rapid, honestly. It really isn't. It takes a while to build. I don't know about you, but I've witnessed how operating systems are built, and it's like sausages and law; you don't want to look.

It takes a very long time. There are a huge number of compromises.

People actually do this. These aren't made by machines. And people have a bad night or somebody yells at them and they come in the next morning and they're coding.

How good is that code that day, really. Have you ever driven a car that was built on a Monday? Don't buy a car built on a Monday, if you can avoid it. It's generally not that good quality.

So, all of these procedures just are indicators to me that we think about it wrong. We think about it not as an ecosystem which has mutually dependent parts, and where failure in one part almost always and necessarily is going to create failures in a different part.

MR. SILVER: Thanks very much.

Vic Winkler, do you have any thoughts here?

MR. WINKLER: Yes, I do. The first one would be to listen to Kathy about the microphone.

MR. SILVER: Excellent.

MR. WINKLER: So, I agree with many of the things that were stated here.

The difficulty for the products and the decision makers really comes when you don't have enough information to begin with, and you may not be aware of other choices, right?

The open source initiative is taking big advantage of that.

But as you take individual products and compose them into an infrastructure, for instance, for a small business or a larger business that manages information about me, I've come to be very suspicious of the level of skill on the part of the people doing this.

I think many of them don't really understand what it is that they're doing.

They've learned about these products maybe just by walking into the consumer stores and these products weren't necessarily designed to be put together in a manner that improves or even maintains a level of security, and that's what we have with sophisticated solutions in infrastructure.

So, there are a number of different levels to the problem, and quality is certainly one.

I take a much more charitable view towards the people writing software, maybe because I work for Sun, right? But all humor aside, writing software is a defective process, and it's not fair to people who are engaged in it to write it off simply as a function of human beings engaged in a human process, although that's quite true.

But what comes out of the process are logical specifications that machines then execute. The tools that we use to write those specifications aren't really enabled to allow for the resulting products to be complete and correct.

Kathy mentioned formal methods before, and I'm a real believer in the need for the software industry to change towards one where we specify the logic and not the code, and where a process that itself has been designed and tested then converts the logic specifications into things that are executed, and then it doesn't matter who does it. The software will either succeed or it won't in terms of its evaluation by the process.

MS. LEVIN: For those of us who aren't technologists, what do you mean by saying let's work on the logic and not the code?

MR. WINKLER: Okay. It's hard to talk as an engineer without slides.

MR. NEUMANN: Could I stick in a word on that?

Back in '73, when we did the fly-by-wire system, it was formally specified in a formal, logically defined language, and we mathematically proved properties about the layering properties, the synchronization, the distribution of information, the voting scheme.

This is a seven-processor system where everything was two out of three voting on the critical tasks, and there was a great deal of formal analysis, mathematically, logically sound formal analysis that showed that the algorithms were correct, the specifications were consistent with the requirements, the code was consistent with the specifications.

So, there's an example.

MR. WINKLER: Yes.

MR. NEUMANN: A 30-year-old example, but it's still an example.

MS. BOHRER: In maybe more layman's terms, if you think of mathematics as being extremely precise and everyone agrees that one plus one equals two, all right? And you think of expressing a policy or directions on how to get somewhere in English to someone and the chances that it would be mis-communicated. Formal languages are much closer to mathematics than programming languages, which are a little bit closer to English.

MR. WINKLER: Absolutely.

My wife and I found that out when we spent about 10 minutes sitting on opposite sides of the living room about a year ago, each thinking that we're talking about the same thing. After 10 minutes, I said, Rebecca, it's astonishing. I don't think we're talking about the same thing. She said what? And we clarified it, and it was absolutely the case. So, the room for error in English and then in programming languages is significant.

As a former software developer, very few times do I see programmers doing anything more than rudimentary testing to see if the code will work as they think it should work versus testing it against unusual boundary conditions or under circumstances that it wasn't really designed to operate under. So, adequate testing is one of the problems.

That's an opportunity for somebody with a great deal of talent or even minimal talent, a hacker -- but there are some wonderful cases of incredibly creative exploitation of how to manipulate a piece of executable code to do something it wasn't designed to do and thereby take advantage. So, this kind of thing has to be reduced.

That's not, however, where most of our problems lie.

Most of our problems do come from mis-configuration or systems that were designed predominantly with functionality in mind without taking care of other considerations.

So, engineering is really last on the list when it comes to most developers, most vendors, and most of the technology that you use.

If you want to continue to encourage the propagation of dangerous code, please continue buying technology that causes most of the problems.

I think that maybe the electronic equivalent of what happens at your firewall on a periodic basis, Frank.

MR. SILVER: Howard, do you have a point to add?

MR. SCHMIDT: Yes, a couple of points, if I could.

First, on the use of quality assurance in software development, this is a relatively new phenomenon, because quality assurance has been changing over the past years. It used to be the two major criteria were does it work and does it break something else, and is it functional. But what we've seen recently is what I see as the paint-by-number scheme when it comes to IT development.

I failed stick figures 101 in school, but yet, I can do a paint-by-numbers thing and make it look pretty good, because all the pieces are there. All I have to do is fill in the blanks, and that's some of the modular libraries that make coding easy for us. If there is an inherent flaw within that particular library, it also becomes an inherent flaw within the application.

The other piece that relates to this, quickly, is the fact that we talked about how IT would make our lives easier. We've actually moved in the realm where, in a lot of cases, we've created a humanization of every IT system to where I've had identical hardware running identical bits on a operating system, and it does different things.

It's almost like the core DNA. You may be allergic to penicillin, I may be allergic to milk, but yet, we're still humans and adults and males and so forth. Consequently, we've seen this DNA-building of the IT systems, which in some cases is very unpredictable, just like it is in the human body.

MR. SILVER: Have we reached the point of negligence actions based on inadequate IT implementations? Does anyone have any thoughts?

MR. PURCELL: It's coming.

MR. WINKLER: Yes.

So best practices are being defined in all different vertical areas -- finance, health care, et cetera, right?

And over time, as these best practices become clearer to not just the practitioners in those areas but to the end users, the patients, the banking users and so forth, I think it's quite clear that the lawyers will take advantage.

MR. SILVER: Tony, I know you have comments on open source for later, but with regard to security right now, do you have anything you want to add?

MR. STANCO: I think I will keep my time for later.

MR. SILVER: All right.

Edward Felten, any remarks here?

MR. FELTEN: Yes. There are two things I wanted to say, although much of what I had planned to say has already been said.

First, although the discussion earlier in the day focused a lot on best practices, benchmarks, and so on, and there's been less of that discussion on this panel, it's important to recognize that best practices are incredibly worthwhile and really foolish not to follow but also to recognize that they'll only get us so far. I think we're going to realize over time that best practices alone are not going to get us to where we want to be, best practices in the use of technologies of the sort that we're accustomed to using, because those approaches are fundamentally reactive.

They react to vulnerabilities that have already been found, that people have already been burned by, and it's a good thing to not get burned in the same way that someone else has been burned before. But it's also the case that new problems, new vulnerabilities, new exploits are always coming along.

The rate of new vulnerabilities being discovered, being exploited, is as high as always, and unfortunately, the speed with which the bad guys can exploit problems is only increasing to a really scary rate. We're going to have to become more pro-active about dealing with security problems, baking it in, designing it in, and that's what a lot of the panelists on this panel have been talking about. That brings me to the second thing I wanted to say, which is that it's important to recognize that all of the talk about better design, better quality assurance is right. That's what we need to do. But it's not the case that we know how to do that at scale for realistic systems -- and we're not doing it.

There really are fundamental unanswered basic questions in computer science that we have to answer before we know how to do real quality assurance on big complicated software systems, and it's going to be a long time before that happens. I think one of the reasons the market is not providing that high level of quality assurance is just that no one is even close to knowing how to do it.

MR. SILVER: Richard Purcell, how do we go about protecting information better? What is the way out of this problem as you see it?

MR. PURCELL: Well, I think Kathy did a good job of laying out a framework that's useful. I think data minimization is one of the keys.

In the off-line world, we're very used to having collected, historically, a huge amount of information for every purpose.

This harkens back to a few weeks ago in the prior workshop where we talked about the example of how technology is so cool that states now can essentially encode your driver's license information more thoroughly onto an instrument, a driver's license, and make it retrievable instantly.

Well, so I want to go to a bar, and I don't get carded anymore. I wish -- but they card me. Fine.

So, when you're carded to purchase alcohol, what is the data point they're actually looking for? And the data point is simply that you're over 21, period, end of story, not who you are, not where you live, not your weight and height, not your picture, not anything like that, simply that you're over 21.

However, the new technologies, the digitization of driver's license information combined with our legacy habit of using a driver's license to collect the age information mean that bars are now scanning driver's license, where possible, and collecting and databasing your entire identity, as well as the time that you came there, perhaps even some sequential number that associates you with other people who are also there, and all kinds of things like that.

So, why? Why are we doing that? Well, it's because we're used to it. It's because we've always done it that way.

So, what we're doing is we're not saying the technology, the digitization, the ability to apply technology to current issues gives us the opportunity to change our behaviors.

We just take the same old behavior and apply the technology, and we end up in these kind of messy goos where there's just too much data. We have the opportunity to undo that.

So, data minimization is one of the keys, I would say, as well as the privacy management practices that are bi-directional, corporate and individual.

MS. LEVIN: Let me follow up with this question, use of Social Security numbers. Historically, we'll agree that they were started for one purpose and now they're used ubiquitously.

You can't even go to a doctor's office now without being asked to give your Social Security number, even though you're giving your insurance number and they're going to pay for it. There have been bills proposed on regulating Social Security numbers, and they're pretty complicated. Some of them talk about authorizing a lot of other uses because we're so used to using them. Businesses are very used to using them for a lot of purposes. It is, I think, a microcosm of the problem.

How do you see us getting out of some of these older systems and yet we realize there's a great need for people to be identified in various contexts? We talked a little bit about this at the last session, about data minimization.

But you have these tensions from government and commercial entities that want the data.

MR. NEUMANN: There is a huge educational problem here.

One is that if your Social Security number and your mother's maiden name and other information that is essentially public record, such as your birth-date, are used as authentication information instead of identification information, there is a fundamental security flaw as a result of that.

Data minimization is part of the answer to that, but I think the burden -- again, maybe we get back to liability.

Anybody who uses a fixed password, a four-bit PIN, for example, that goes in in the clear and can be shoulder surfed, if you will, or photographed is vulnerable.

One of the most secure cryptographic devices that was created for public use was the clipper chip. The PINs on the clipper chip went in in the clear, and the idea that this is going to be a super secure system was, in that sense, a joke.

So, again, it's back to this oversimplification. We stick our head in the sand and believe that all of the stuff that we've been using is fine, and yet, we have practices -- this has nothing to do with the technology, in a sense.

It's an administrative thing, the idea of using a password that is going to protect you, even though it's flying around the Internet in the clear or it's being given over a telephone, or a Social Security number that's used as an identifier, which is being used in the clear over the telephone.

This is a very foolish way to run a business, and I think there is a fundamental need for things like cryptographic tokens, for example. Then we get to PKI and then we'll open up another hornet's nest, because Carl and various others do not believe that PKI is a sound way to base an infrastructure, and yet, this is what is being done. The same thing can be said for SSL.

If the operating systems on which you're building your castles in the sand are fundamentally flawed, then your whole environment, your whole enterprise is potentially fundamentally flawed.

MR. SCHMIDT: Peter and I are in complete concurrence with this, because when you look at digital identities or PKI, which is something we've been very, very slow to move to -- I mean two-factor authentication is long overdue.

We have multi-levels of two-factor authentication, and for those of you who may not be familiar, two-factor is something you have such as, in the case of my military ID card, a smart card chip and a PIN number, something you have -- or something you know, which means they have to put the two things together. This is very, very rudimentary, it works perfectly, but yet this has been around for a couple of years. I lament every time I go to a military installation or a government agency, I have yet to find a terminal to plug this thing into and utilize it.

We have it, the technology is there, but I have yet to find anywhere, including some of the offices that create these things and issue them.

So, consequently, when you look at it from a societal standpoint, that is one way we could go.

Once again, not everybody is going to be sophisticated enough to be able to walk in, get their card, understand that there's a level that is totally anonymous that gives them access to health care information that they may have concerns about, all the way up to INFALC on occasion so you can transmit security clearances for government meetings.

There's various levels we can provide, but what happens, every time we have a conversation, it's too difficult, the unsophisticated user won't understand it, so we do nothing.

MR. NEUMANN: And then the dependence is on the high-tech solutions. For example, the smart card, which is seemingly a high-tech solution, is itself vulnerable. We have friends in the community, good friends who are good people -- Paul Cotcher, for one, various others -- who have broken essentially every smart card that exists today, extracting the secret key out of the smart card in a very short time, but yet, a lot of technology will be built on that concept.

MR. SILVER: Let's talk now about convenience and the importance of convenience.

Alan Paller, is this something that's going to possibly lead us out of this problem, at least in part?

MR. PALLER: Clearly, building security in so the user doesn't have to be an expert and the system administrator doesn't have to be an expert is an essential first step. That was in the first panel in May. Nobody disagrees with that, I don't think.

A few panels ago, we had a member of the panel who, in an earlier life, sat in his dorm room at college and broke into systems and stole things and was really a bad guy before he figured out he could make a lot of money acting like a good guy. I thought it would be useful to take people very quickly through what he would do to old people's database and then what technology would fix that real quick.

I just think it would be a nice way to pull our discussion together.

So, he wants the Social Security numbers. He wants some other stuff, too, because -- there are lots of reasons to steal people's data, but the one you can turn into money fastest is credit card numbers, because they sell for between 20 cents and $1.40 depending on whether you also know that three-digit code that you're never supposed to put in the computer and the expiration data. He wants other things, but he wants their credit card numbers.

So, how's he going to get them? I'll just take you through.

He's lazy. Not lazy. He wants to find the easiest way of attacking.

So, the first thing he does is he knows, as Peter said, the operating systems are fundamentally flawed. There are actually two problems in the operating system.

One is they had mistakes in them.

A CIO from one of the Federal agencies was sitting at Microsoft, and Balmer bounces in the room, and news had just broken about another buffer overflow, and he says damn it, I thought we'd figured out how to fix that problem years ago.

So, the operating systems are fundamentally flawed because the programmers make errors -- that's a small problem.

The big one is they're fundamentally flawed because people install them configured unsafely, and they do that because that's the way their friendly vendors told them to install it.

There's no end user stupidity here. That's how I got it from my vendor.

So, the first thing I do is I just check to see if any of the common vulnerabilities are there, because the common services are there. I do a real quick check. No trouble. I'm in.

Okay.

So, that's the easy one. I get by that one.

Maybe they've configured it right so I can't get in that way.

Then I decide, well, all right, they've got a database accessible, meaning I'm a user, I want to get into the database, attack, the same thing. The database people make mistakes in programming, and even worse, they make mistakes in configuration, exactly the same as the operating system people.

So if I can't get in on the operating system, I can come in at the database, and the third level would be the application.

I could do both of those attacks at the application level.

I want to say something about configuration.

We expect the system administrators to configure the system safely. All of you who work in large organizations hire people to do that.

Just a short time ago, one of the largest system vendors was running a training class for law enforcement people in Washington. On the night of the first day, the guy who paid for it walked in and said this is great, we love learning how to run the systems, but what we really want to know is how do people break in and what should we know about blocking those kinds of problems. Because you are the experts, you're the people who would know, please teach us that.

He said I'll come back and tell you by 10:00 in the morning.

He came back the next morning and he said it is corporate policy not to teach that to students. This is one of the largest vendors.

It's true of all of the vendors.

If you have a person who has a certification from the vendor in system administration, he has never been taught security, never.

To the extent he has been taught security, he's been taught how to run the for-sale security products that that company sells but not how to secure the basic operating system.

So we have a situation where we're expecting people to do things that they can't do.

So that's why Dell's move is so important.

MR. NEUMANN: There's one other fascinating problem there.

IBM is doing a phenomenal job in their autonomic computing program -- that is, a system that basically doesn't require a lot of system administration, because it's going to keep on running no matter what happens to it. It's going to diagnose the fact that it's under attack and reconfigure itself and so on.

The problem there is that suppose you get rid of all your system administrators, or most of them, and they get lazy because things don't go wrong anymore, and now something breaks.

You're in real trouble, because you have either got to out-source your critical system administration to some third world Beltway bandit subcontractor or you have to have a guy on staff 24 hours a day on call, or a team of people, who could come in and be skilled enough to repair the system under conditions that you've never seen before.

MR. PALLER: Yeah. Nothing I was trying to imply said that you don't still have phenomenally skilled system administrators.

It's just you can't expect all of your system administrators to know how to install it safely in the first place. That's what I'm saying is the error.

We have to train the system administrators. We have to get them up to speed, because they're going to have to deal with new problems as they come up. But day one is where we shouldn't make every single human being who ever buys an operating system from anyone be a security expert. It ought to come out of the box safely, and the idea that it doesn't is malpractice.

I mean it's just stupid, and they've known it for years.

Sorry.

Okay.

So those are the easy attacks.

Let me give you an attack a lot of people don't know about.

We're still stealing their credit card numbers.

Now, this won't work at eBay, because they know how to solve this problem, but there are places where this will work, like 100 or 200 thousand other places.

It turns out the person who sold you the storage devices on which you put the data in the database is not the person who sold you the database or even the person who sold you the computer.

This is the guy who sold you this raid box or the switches and the storage devices that you stick it on.

So it's the hardware, the servers that the data is on, all right?

Well, it turns out that a lot of them have a dial-up port, because they want to make it easy to maintain it, because up-time is the single most important thing. So, they have a dial-up port, and some of them have a dial-up port that has no password on it, and the ones who do have passwords on it have known passwords on it, and you wouldn't want to change the password, because then the maintenance guy couldn't get in, all right?

So, what's the general solution to that problem? What's the general solution? Encrypt it, so that even if they get the data, they can't -- that's why Howard doesn't have the problem, I hope. So that even if they get the data, they've got to go to some of Peter's best friends, and if you make the price high enough to break it, you'll lower the barrier.

MR. NEUMANN: I've got a story I've never told in public, and I think it's time.

Probably 18 years ago, I went up to Alyeska in Alaska and did a security review of their pipeline control system, and I discovered that every node in the network used the same dial-up password for their switch in the router -- I should call it a router, I guess, but it's a one-way router, and it was the same password that was being used by the vendor everywhere in the world.

MR. PALLER: That problem is not limited to Alyeska. Cisco classes teach you to use one of two passwords, which I won't name, and almost everybody thinks because it's in the manual as an example, that they should put that in their routers.

So, those two are in some reasonably large percentage of all routers.

Okay. Two more quick ones, and then I'll get out of here.

Say you've got the systems and they're okay, the hardware and the software and it's okay, but you still want to get in.

The organization has set up, because it's smart, a VPN that allows people to work at home over the Internet, but it's all encrypted channels, so it's all safe as can be.

Most people don't understand the VPN is not a security system. It's a pipe. It's a pipe with a hard wall. The hard wall is the encryption. But if the PC at the other end is used by the person's teenage children, what are the odds that it has a file-sharing program on it with access. Once you have that on it, the VPN is a pipe into the system, and you are a validated user of the system and you've gone around all the things. If that doesn't work -- and say I really do want to get into eBay -- then what I'd do is I'd spoof an e-mail message from Howard to 50 of his system administrators.

"Spoof" means send them a letter with the return address on it that says Howard Schmidt and you can do that really easily, really easily. So, you send them lots of e-mails, and they all say, wow, my friends at Microsoft -- everybody knows he used to work at Microsoft, so "my friends at Microsoft" sounds right -- just told me there's a big bug in Internet Explorer and we've got to get it fixed. They haven't made it public, but they've set up a special web-page for us to download the patch. Click here.

Well, the "click here" works. It just doesn't take them to Microsoft.

Would this work?

MR. SCHMIDT: No, because everything I would do would have a digital signature. It would not. But in a lot of instances, though, you are correct.

MR. PALLER: And that one takes training.

So if we fix everything on the hardware and software side, we haven't fixed more than 50 percent of the problem.

The other 50 percent of the problem is I can fool you into opening that. Almost no one else uses digital signatures, even the guys who sell them. So, I can fool you into going to a website thinking you're going to Microsoft, download a patch, put it on.

That patch actually opens that computer, bypasses the firewall, and the computer goes to a website looking for commands. So, you're not getting in, it's going out.

There's absolutely nothing to stop it.

Those are the ways I would get you. There's technology fixing all of that stuff.

MR. NEUMANN: I had a wonderful thing in my "Inside Risks" column from some Russian guys who pointed out that if you put the "O" in Microsoft in cyrillic instead of in our alphabet, it was indistinguishable, because the "O" is identical in appearance on the screen, and so, microsoft.com with the cyrillic "O" gets you a very different website than the one you'd think you'd get to.

MR. PALLER: That's a hard one to fix.

Okay.

So, just quickly, what Dell's doing is absolutely the most important stuff that's happening. We have to have that kind of configuration baseline in every application, every operating system, every piece.

The other reason Dell's work is so important -- and it is the one that people miss -- is that a lot of the reasons the operating system can be broken into is because the applications force you to undo security, meaning the application was written on an unsecured operating system.

So, if you want to install that application, you are forced to make your computer un-secure. Even if you installed it with Dell's technology you have to turn it off. IBM's got some products that do this to you, because the developers wrote it for an unsafe version of Microsoft or for Windows.

You want to do that, but the guy wrote it for the system the vendor sold.

Once Dell starts selling a system that people say it’s a safe configuration, then buyers can say I'd like to buy my applications and I want you to certify that it runs in a safe configuration, but until somebody as big as Dell or as big as Microsoft makes that kind of move, nobody can act sensibly, because they don't know which configuration to match to.

It's a wonderful year for progress.

The vendors are really doing a lot of work.

They're making some moves that are purely pecuniary.

Like Microsoft does this thing where they'll automate a patching, which is absolutely essential for all of the grandmas in the world, but they won't do it for anything you already have. You have to buy their new operating system.

So, it's pecuniary, but it's moving us forward in the process. If people want to know more, I'll be happy to fill in all the good things that have happened, but it's been a very good spring for improving, not getting us around the fact that we still have problems, Peter.

MR. SILVER: Tony Stanco is here to talk about security, privacy and open source.

MR. STANCO: Actually, I guess it's appropriate that I'm going at the end, because open source is almost a parallel universe that really doesn't touch a lot of these other places.

I'm going to talk a little bit about open source, which is really a completely different way of doing things, and like the flight of the bumblebee, it really should not be working, except it is.

Open source is gaining momentum around the world. Basically, all the major companies have some kind of open source strategy.

This isn't a coincidence, because Wall Street requires it.

They don't, they actually get penalized on Wall Street, and if you've got a mixed message, you get penalized, too.

Europe, China, India, South America -- they're probably ahead of the United States. The United States has the risk that it might fall behind, except just last week, DOD issued the first, for the Federal government official policy statement. It’s in the package.

It was dated May 28th, and it really just got off the press yesterday.

What the memo does is just basically level the playing field between proprietary and open source. So, the government isn't picking on anyone who's here.

That also shouldn't be very exciting or surprising except because of the lobbying that's been going on for the last couple of years. Ptech October 2000, basically said the Federal Government should level the playing field for open source, except between then and now, there's been a lot of activity, let's say, at the political level.

Also in the package, there's a Mitre report on the use of free and open source software in DOD, and what it said is that if you try to yank out open source from DOD, you basically lose your security. It actually is even stronger than that. It actually says you can't plug into the Internet, because most of the Internet runs on open source software.

So, open source is important. That's the basic message there. Open source security.

All right.

NSA -- I'm sure everybody here knows about the NSA. They started a security-enhanced LINUX project, SC-LINUX. NSA has been worried about the critical cyber-infrastructure for a long time, but really, in the last decade, they were very concerned.

In fact, they're concerned that there isn't even a secure operating system, and you need to start at a very fundamental level.

What they tried to do is they have this architecture, mandatory access control that's used in certain military installations. They tried to give it to the proprietary companies about 10 years ago. Before

9/11, there wasn't a market for security, as some other people have mentioned. So, nobody adopted it.

The technical people thought it was a great idea. The marketing people said it's a cost center and nobody is going to pay for it.

So, it didn't work. It didn't get vectored into any of these mainstream products.

So the NSA said, hey, let's give it to the open source people; maybe they'll take it.

Well, they took it, and there's a lot of activity in the security enhanced LINUX through the open source community, through the university where we are through a lot of universities around the world, in fact.

All right.

Let's talk a little bit about security. Security really is still very misunderstood. I think there was a sense at this event that there's a lot of ambiguity and a lot of misconceptions.

I've heard some of the same things here.

I was at a CIO council web services working group meeting just recently, and they talked about securing the web services applications. And they didn't worry about anything below the stack. But the NSA has made it very clear that you really need to start as low as you can go, because otherwise, doing it at the web services level, you're really talking about bulletproofing the third floor of your house and leaving wide open the doors and windows of the first and second floor.

In fact, there's an NSA colloquium on secure systems going on this week, and there was somebody from Australia who said forget about the first floor. Threats to security are working below that. They're going to the real foundations. They're working in assembly language. They're working at the hardware level. They're working at the BIOS level. So, if they want to get you, you can even have a secure operating system, and they can get you.

But the point is that's a good place to start. That's a nice dividing line, because that's where the software starts, for the most part.

Unless we get at least that low, nobody should have a sense of security. It's all smoke and mirrors. The vendors will tell you that it's secure. They'll tell you that they have great products. But you know, they're just selling you products.

MS. LEVIN: Tony, you're saying the level you would start out would be the operating system?

MR. STANCO: That's what NSA said.

QUESTION: The BIOS?

MR. STANCO: Yes, you should, but let's start with the operating system. You can always go lower, but that's a nice place to start, and that’s where NSA wants to start. That’s what they're trying to do with the SC-LINUX.

They're trying to get the secure architecture up there.

All right.

Let's talk about open source security. I'm not here to say that open source security is going to be any better than proprietary. There's no definitive study. I'm not going to make that claim.

You know what? It doesn't matter anyway, because they both aren't good enough.

Security is not something that is baked in, as somebody said, or architectured inside the development process, and this is very key.

Neither open or proprietary is doing a very good job.

The good news is both are starting to look at it. SC-LINUX, a lot of the proprietary companies -- Microsoft, IBM, Sun, Oracle -- everybody's looking at security at this point.

The bad news, again, is that none of these are going to be usable products for the next three to five years, as somebody mentioned, because you have traditional product cycles that really rev about that speed.

All right.

The other good news -- and there are some pieces of good news -- is that there's some other things happening -- Common Criteria -- NIAP, which is the National Information Assurance Partnership between NSA and NIST. They require at this point, as of July 1st last year, though there's still some wiggle room since there wasn't enough product in the pipeline, that sensitive software, military systems, has to be evaluated and certified.

Now, this is good news, because once they basically debug the process, the CC-NIAP process, everybody expects this to go to the civilian side of the government and then to everybody else, here and international, because at CC, the common criteria part of that is really international. So, the future is starting to look a lot brighter if you have a far enough horizon.

But let's leave all this aside, too, because open source is different, and it really goes to fundamental ideas of not only technology but society and organizational structure.

The bigger question that I want to raise here that I don't think anybody else has raised is who do you want to protect, who do you trust to protect citizens? Are you going to trust companies? Are you going to trust government? Or do you have to find somebody else? Is there another group?

Well, let's talk about companies. They have fiduciary duties to maximize profits for shareholders. That's not a bad thing. I used to work for the Securities and Exchange Commission. I mean that's a good thing, right? They created a lot of wealth in the last 300 years. But we just have to realize that their mandate is not to protect consumers or citizens.

Now, the theory, how the free market relates to societal benefit is that free market competition among the companies checks the ambitions of any one particular company. So, the competition and the market regulation has, through this competition mechanism, achieved the societal goals.

So, you have this invisible idea. I'm not saying that's wrong, because we know it's right. You can't say that it didn't work.

You have eastern Europe. You had East Germany. You had West Germany. I mean, come on, same people. The only difference was the legal system and the ideas, the principles of free markets and democracy.

So, there's a real test case there that says this -- there's something there.

But the key point is you have to have a dynamic market. You have to have the competition. And software has network effects, especially once you get to the Internet. Hopefully, everybody knows what network effects is.

The value of the system or the product increases exponentially with every person who gets added to the system.

So, that creates monopolies. It creates situations where a particular consumer cannot choose, because you could choose to unplug from the electrical grid or you can choose to unplug from the phone system or you can choose to unplug from the computer infrastructure, but you don't have choice beyond that. The choice is in the system or not in the system.

Market regulation -- we can probably cite two or three cases that point this network effect out in the antitrust area.

Let's just assume that markets aren't sufficient. We don't even have to conclude that. Let's just assume for argument's sake.

So, what happens then?

We can't look to the governments -- to the companies, let's say. Can we look to the government? Well, the government usually steps in. That's the usual solution when there's a market failure. But in the past, government stepped in in slow-moving capital-intensive industries. So, you generally regulated the assets, which is feasible.

But software, IT -- that's not how it works. It's a fast-moving, innovative industry.

Industry will always, in my opinion, outstrip government's ability to do oversight. They have more assets. They can incentivize. They can give stock options to even the best in the government to bring them into the other side.

Can government really provide effective oversight when it relies on industry, in the first case, to constantly innovate?

Again, who do you trust to protect citizens?

The problem actually gets a lot worse. If that wasn't bad enough, it actually gets worse, because software in cyberspace is functionally equivalent to law in physical space.

Basically, law regulates interactions between people, between businesses and people, between businesses and businesses, between people and businesses and government. That's really what all the rules are all about.

Software does exactly the same thing in a cyber world as that, exactly the same. You will interface not with people directly but through your machine. People are already talking about these mobile agents that go out and actually do the contracting. There's a real indication that this is not completely out in left field.

These agents are supposed to set up your contracting terms, and go out into the Internet and actually execute the contract.

So if that isn't law, I'm not sure where we're left.

Let's extend this a little further. Let's say we can arguably say that it's like law.

Now, the creation of law, as everybody here knows, especially in this town, is a very complicated organization, carefully structured with checks and balances, because it's fundamentally too important to society, too important to democracy, to free markets -- it's the most basic layer.

So, we have legislatures, courts, executives, executive agencies, the legal profession, legal schools, political journalists. We have think tanks. As somebody mentioned, there’s this ecosystem that, works out the legal rules.

So, if software is like that, where are the checks and balances in the creation of software for protecting the consumers and the citizens?

And if you look at it from this perspective, do you really want to leave it to the market, which doesn't seem to be able to control the appetites of business in the first place?

You can obviously have a company -- if we thought it was such a good idea, we can have a company, for efficiency reasons, create our laws.

Why is that different? Why would we not accept that?

If we leave it to the government, is that a good idea? Because it's a fast-moving industry. It’s not clear that they can do it.

What I'm saying here in this roundabout way is that the issue may not be at the level that was proposed in this panel, because the question might not be how do you design technologies to protect consumer information at this particular time or at this particular place, but it's probably fundamentally how do you design a system that will design technologies, that will protect consumers, because the dynamics of the environment are such that a solution isn't going to help. You need a system that will adapt.

If you leave it to the industry and if you don't want to go down this road, these institutions lack the checks and balances. I would suggest that you're constantly going to be where we are, which is always behind industry, trying to catch up.

Industry is going to exploit and harm consumers, and there's going to be an outrage at some point. They take a lot, but at some point, they become upset and they complain, and then policy people like the people in this group, like myself, come up and try to find a solution for that problem.

By the time we cycle through that problem, industry has said fine and they're off to the next problem and the next exploitation of people.

It's not a problem of a technology. It's not a problem of policy. It's a problem of structure. And unless we solve that problem, this is an ongoing thing.

All right.

I'm here to talk about open source. Where does open source fit in this?

Well, like open government and transparent law creation, as a first step, you would expect, if software is law, that you would need open inspection of software. But I'm not going to say that open source at this time has the necessary checks and balances to protect citizens.

Yes, it's better than companies, in my opinion. Yes, it's more capable of government, because they're technologists that obviously can duke it out with all these companies on the same terms. But it still lacks, for a system, the appropriate accountability that society would require for legitimacy. The appropriate accountable structures still need to be created even if you're using open source.

But realizing the past responses, what we've done in the past, how we've looked at things in this new cyber-world, it isn't going to work.

That is, itself, a first step. Open source, in my opinion, is a partial answer. It's a starting point. But you really need to get to the point of thinking and laying out and designing accountable open source development systems.

That's where the time should be spent, in my opinion, not designing, as I said, the particular policies of the moment and not just trying to play catch-up with industry.

So, that's where I'm going to end.

MR. SILVER: Dr. Neumann, any comments on open source?

MR. NEUMANN: Yes. That was quite a speech.

Let me make a couple of comments.

One is that you're absolutely right. Open source by itself is not a panacea.

Without the things that seem to be not present in the proprietary development process as much as they should be -- namely, attention to system architectures, attention to good software engineering practice, avoiding some of the problems of legacy system backward compatibility with every system that's ever been built in the past or monster cut-overs through architecture for distributed systems -- one can achieve, I think, very high security reliability and so on. But that applies to both the proprietary world and the open source world. Without that, it is very difficult for us to have the kinds of systems that we need.

Now, your argument is good in the sense that the open source world has an opportunity to do things that are much more difficult to do in the proprietary world.

I'll give you one example, the DARPA program called CHATS, which is Composable High Assurance Trustworthy Systems, of which I happen to be one of the contractors. It is purely open source. Everything in it is open source. It's taking LINUX VSD variants --

MR. STANCO: We're part of that, too.

MR. NEUMANN: -- and making some truly considerable improvements in what can be done in open source by itself.

But without the discipline that is required to develop systems, the open source thing is not going to go anywhere either, and I think --

MR. STANCO: Can I respond to that?

MR. NEUMANN: Yes, sure.

MR. STANCO: Granted.

But I'm just not sure how using proprietary methodologies solves the problem.

In fact, I would think if you have open source, you teach open source, you teach architecture that bakes in security to the students, who then go out in five, 10 years and implement that, you're in a much better position than having students work on a closed system, a black box, you know, click here, click here, click here and it will be secure and go out and work on that.

MR. NEUMANN: I agree.

The point I was going to make was, in fact, the exact opposite, that the stuff that has come out of the CHATS program -- for example, some of the tools that came out of my project done by the Berkeley team for finding all kinds of security flaws based on formal methods, oddly enough, are perfectly applicable to proprietary software, as well, if only they would use them.

MR. STANCO: If only they would use them, exactly.

MR. NEUMANN: Let me finish my comment.

Multi-level security was mentioned here. I want to point out that there are some potential open source solutions to multi-level security that the marketplace has not picked up on.

One is work we did back in the '80s on showing how you could put an off-the-shelf Oracle on top of a security kernel and the result is an A1 -- effectively, a very secure multi-level secure database management system without having any trust in the database management system for security.

MS. LEVIN: Peter, why did the marketplace not pick up on that?

MR. NEUMANN: Well, Oracle discovered they could do something on their own.

We worked with Oracle, actually, on that, and they discovered that they could modify their kernel a little bit and come up with something that was multi-level secure. Nobody wanted an A1 system at that point. It was not practical. It cost too much to develop it. And the evaluation procedure was so complicated that it took years, and by then your software had gone many levels beyond it.

There's an architecture that Norm Proctor and I came up with in 1992 on how to build multi-level secure environments out of single-level components and some trustworthy multi-level servers.

So, all of the trustworthiness is in the servers for multi-level security. That's something that can be done essentially off the shelf, with a few open source trustworthy servers and anything else you want to use, and you actually can wind up with a multi-secure environment.

The tools that have come out of the CHATS program I think are very important and very applicable to open source, but they're also applicable to proprietary stuff. The key argument comes back to the question that we raised earlier of whether the research community is having a real influence on the marketplace, and I think there may be arguments. Howard made the case that, in fact, the marketplace is becoming much more aware of security.

Certainly, Microsoft has made a huge effort in the last year-and-a-half. They spent, what, 1,200 man years in February of last year alone, although maybe some of that was just a half-day course on how to make secure systems, I don't know. But the point is that there is a need for a cost-driven marketplace where there is a real incentive, whether it's financial or jawboning or whatever, to the mass-market software developers to produce stuff that is much more robust.

If you look at the buffer overflow problem which was mentioned earlier, buffer overflows have been around for 30 years.

We've known how to get rid of them for 30 years, but they are pervasive, and they keep appearing and reappearing and reappearing. CERT keeps showing that half of the breaches in securities laws over the past four or five years are attributable to new buffer overflows. They keep recurring.

But we know how to get rid of them by using intelligent architectures and intelligent software and intelligent use of programming languages and programming style. It's easy. But it's not in the interests of a marketplace whose primary goals are not to develop secure systems.

So, if that's changing, I welcome it, I think it's wonderful, but it's a very slow process.

MR. SILVER: Are software development contracts being written at all to shift risks to the developers in case of security breaches?

MR. NEUMANN: Ed would be a good one on that.

MR. SILVER: Professor Felten.

MR. FELTEN: Actually, I think someone else on the panel would be best equipped to answer that.

MR. SILVER: Go ahead and make your remark. Maybe we can save the question for later.

MR. FELTEN: I just wanted to amplify a little bit on the point Peter made about buffer overflows. As he said, it's a very common category of bug. It accounts for half of the CERT advisories, and it's a problem we know how to solve. Yet, both proprietary and open source software is still rife with buffer overflows. This should be telling us something, that, in fact, there is an awful lot of inertia in the software development process and that it's not the case, I think, that industry has been lax in picking up the knowledge that does exist about how to develop more secure software.

I think it's just much harder to transition basic knowledge about security into practice and especially into the software development process than many people realize. I think that although it's true that commercial software has not improved all that much in security, that's more a reflection of the fundamental difficulty of improving security as opposed to anything that's broken about the process itself.

MR. SILVER: Tony, then the last word to Alan.

MR. STANCO: I'd just like to respond to Peter on four basic points that he brought up, or themes.

Okay.

The research community -- it seems to me that open source follows the scientific method of allowing everybody to share code, results and experiments and everything else.

I don't see how there's a conflict with open source. It seems to be a reinforcement. It seems to go back to first principles. And I'm reminded of a story where people didn't used to share ideas.

In fact, a few hundred years ago, heart surgeons didn't share their techniques, and society at some point said, you know what, I don't think you should die with those techniques, because there are other people who can be saved. Maybe this is the same; maybe it's different.

You talked about coexisting, I think, or one or the other.

I'm not sure this is an either/or situation.

I think the government, as a policy, should say it’s a level playing field, which is what the DOD memo said. I'm not concerned about it.

I personally think that open source has been under-estimated from its beginning.

People, 10 years ago, never would have imagined it would get where it is, and I think they're still under-estimating.

So, I'm not concerned about a level playing field. I'm concerned about de facto or de jure prohibitions. But if we can level the playing field -- for example, de facto would be that procurement officers must consider allowing is open source software procurement. A lot of the software lobbyists were being dropped into state legislatures to oppose procurement officers from even considering open source -- not just buying it.

You talked about security and I talked about the fact that there's no definitive study between open source and proprietary that would sway people, reasonable people one way or the other, but there's still anecdotal evidence that open source is more secure.

What is this? Basically, every military establishment around the world uses open source. They don't trust proprietary.

Now, there might be a lot of reasons for that. Some of those might be social reasons. Some of those might be nationalistic reasons. But those are still security issues.

Let's pick on one of our enemies, like France, and you're not sure if NSA sees all your documents. From France's point of view, it's a security problem if there is something in there that redirects all your information.

And the last thing -- I think this is a very valid argument that you brought up, the business model. I don't think you called that a business model, but you said these people have to be paid or something to that effect. Otherwise, there's no incentive.

That I agree is very important, though I have a lot of faith in the free enterprise system, the free market system.

I think if government stays out of the way and says everybody play this out, things will rise to their appropriate level and bad solutions will fall to their appropriate level.

I think, yes, business models are currently lacking from open source, but I also think that people are working on open source business models. I actually think that they're going to develop them pretty quickly, because this reminds me of what happened with LAN's and the Internet. The same arguments, right, that you can't use a public property Internet to really do anything. You've got to buy up proprietary LAN's, because you need to have incentives. You need to have a company behind these solutions. Who is going to support a public good Internet? Well, that's not how it worked out.

MR. SILVER: Alan, you had a comment?

MR. PALLER: Yes. It was in answer to the question you asked.

MR. SILVER: I think you and Howard both had responses to my question on contracts.

MR. PALLER: The question was, is anyone doing something contractually to require --

MR. SILVER: Right.

MR. PALLER: -- safer systems, and the one example that I know about, although I've heard of four -- I just didn't write them down.

The one I know about is Virginia Tech has required for the last year that every software vendor that sells them a software package certifies that that software package has been freed of all 20 of the 20 most common security vulnerabilities, and of 620 vendors, only two have not been willing to sign.

Probably that means 300 are lying, but it definitely is a method. The reason I wanted to make the comment wasn't just to answer the question. I think that's the lever.

If you wonder how are we going to get more secure systems, given what Dell is saying, that customers are actually beginning to ask for it, there is one software vendor, big software vendor, that just rails against benchmarks, just, oh, no, we don't want that. Everything's different. The whole world is different. Everybody's different, therefore no security benchmarks.

And one of their customers came to them with $100 million and said we want to buy a lot of your software, but only if you'll deliver it according to these benchmarks. Oh, sure, absolutely.

I mean publicly angry about it; privately, of course we'll do it.

And I think that's the lever. As Dell proves the vendors can do it, as the customers prove there's a market for it, I think we roll over, and then the other really wonderful thing is at the FTC.

People are now promising security. The FTC has a spectacular role in saying if you're going to promise it, please deliver it. I think that combination of the market moving and the FTC saying put up where you said you were putting up is really wonderful, and thank you for running this workshop.

MR. SILVER: Howard. Then we'll take questions.

MR. SCHMIDT: I didn't know there was a "please," but thank you for doing it anyway.

A few quick points.

One, yes, there are a number of instances where there are contractual agreements, service level agreements, whatever capacity you want to call them, that say you will do this certain level of security, and if there's a failure, you will notify, you will contact. There's a whole plethora of issues that are going into contractual agreements now on that issue.

A couple of quick points on Tony’s remarks, and I have a tremendous amount of respect for Tony although I disagree with a lot of what he says.

On the market forces, there has not been a market failure.

If there was a market failure, the government would have stepped in. There has not been.

The market has shifted. The market has corrected. The market is doing a lot more but once again, as I think we're all in agreement, this is not a motor boat we're turning around. This is a 600-foot tanker we're turning around to get these things going.

Also, the National Information Assurance Partnership (NIAP) doesn't do much to level the playing field.

NIAP is very expensive. It's very time-consuming. Only the big companies have the ability to participate. They do a tremendous job. It's very valuable. But we were called when I was at the White House as the President's Special Advisor for Cyberspace Security to look at NIAP and see how we can make that a better tool to improve security.

And lastly, the evolution of things -- I remember back in the early days of CPM, for example, there was a lot of free-ware that evolved into share-ware that evolved into commercial software.

So, what may be an open source today indeed may be proprietary and commercial software later on, which is not a bad thing.

And in closing, it's tough to have it both ways, Tony.

Either the government needs to be in or the government needs to be out.

If the government creates a playing field, that's government intervention in what I think a free market economy should do.

On the other side, you said the government should not be be meddling in these things, and I truly believe that's the case.

The government should keep a hands-off approach, provide some technology, and provide some research, which is vitally needed across the board to make this better.

Thank you.

MR. SILVER: Thanks.

MR. SCHWARTZ: Can I just ask a follow-up question of Howard?

MR. SILVER: Sure, one quick one.

MR. SCHWARTZ: At the beginning of this, you were saying that, contractually, a lot more companies are asking that when there's a breach, that it be known. How much of that is due to the California law and how much of that happened before that law? Were we moving that way already, or has California law pushed that over the edge?

MR. SCHMIDT: I don't have any hard numbers, but from what I've seen, this was taking place long before the California breach occurred, because companies were looking at this issue, as part of the business process -- I need to know these things.

I know I was working on these issues two years ago. If we do a joint venture, business partner, merger and acquisition, that was part of the criteria for establishing the arrangements.

MR. SILVER: First question, please.

QUESTION: Vincent Schiavone, from ePrivacy Group. I had a couple of points to make. First of all, I think we've done a little bit of a disservice here today to answer the question, designing technologies to protect consumer information, to get into a religious argument about open source and closed source.

When we talk designing systems, designing closed systems, proprietary systems and open source systems, there's some basic fundamentals that we did not discuss today.

When we look at technology, technology is not what makes things secure.

Technology can enable us to monitor security. It can enable us to enforce policies. But there has to be the requirement for secure systems and accountability, trust and accountability of consumer information.

Right now, you can build systems much more securely than we are building for consumer information. There is no accountability required for tracking information as it shared outside of the systems, okay?

That's the fundamental nature, and the question comes down to should it be designing technologies or are we going to require technologies to protect consumer information?

Some will argue that we already have the laws in place to do that.

Two examples I'd like to talk about.

One is standard of due care and how this plays in software development.

We heard an example today about spoofing of e-mail addresses.

We have eBay and ex-Microsofters up there.

It happens every day of the week with very large companies.

We're talking about corporate identity theft. We're talking about individual identity theft. We're talking about real theft and fraud. Yet, there is no requirement that they use the systems that have been around, as Peter said, for many, many years to make this trustworthy and accountable.

So, we can't design a trustworthy system until we require that there be one built that handles consumer information.

The other point I'd like to make on standard of due care is that after events happen, how are we holding people accountable?

The FTC has a role. Technology has a role. Best practices has a role.

But until we have a standard that's acceptable and required, there won't be a change.

Bits are bits.

When we look at technology for security, some of the best security is in digital rights management. We have new things coming out that can protect my song across the Internet so Richard can't copy it and share it with Tony. This is very interesting technology.

Yet it's not being applied or being required to apply to our personal information that is no different than the song.

So I'd like to ask the panel, where does standard of due care fit in and requirements for designing systems securely?

MR. SILVER: Who wants this one?

Go ahead.

MR. FELTEN: I believe pretty strongly that the approach you suggested of using digital rights management technology is the wrong way to go for privacy. The reason is that digital rights management technology, although it's loudly promoted, doesn't actually work very well, and it never has, and for fundamental reasons, I don't think it will. I think it's a mistake to think that we can rely on technology to keep someone who wants to use information maliciously from doing so.

I don't think technology is able to do that, and I think it's a mistake to try to use technology in that way. It's particularly a mistake to require people to do so. If we were to require that, we would be requiring people to use a technological approach that I think is doomed to failure.

MR. SCHIAVONE: We're currently now at zero security on much consumer information and not ideal security on digital rights, but from the baseline to where we can get with privacy rights management and how there must be an audit trail for information sharing, it is just very far away from where both ends of the argument are.

MR. SCHWARTZ: Kathy gave a whole list of new technologies that are being built in exactly that area. I mean I don't think it's that far away. One thing that came up is the idea of a vocabulary and how we need a more robust vocabulary than we have today to make that happen, though.

MR. PURCELL: One last comment on this. One of the things that I'm concerned about here -- I'm here for the people.

We have a long and robust history of security specialization and training.

We have no history whatsoever for privacy specialization and training.

We'll hire just about anybody off the street and put them in charge of a database. One of the reasons system administrators aren't very good at their job is because there isn't a lot of training.

Neither is there a lot of hiring rigor that goes into that kind of personnel work and resources.

What I'm concerned about more than anything else is where are the credentials for the people that are handling this data?

We don't have a credentialing program that is very useful.

There's some for security. It's basic, but it's there, it’s something.

There's nothing for privacy.

One of the questions that I have is who is accountable?

And isn't, in some sense, the personnel department, the HR department, somewhat accountable for hiring people and training them, who actually have skills and experience and knowledge about what the hell they're doing, which I don't think is happening.

MR. PALLER: I think the safeguard program actually specifically requires that. They're not doing it, but we can start getting that.

MR. STANCO: Can I just make one comment? Because I think you brought up something that's terribly important, the standard of care.

I think this is a line of argument that will do wonders, because why don't we have a standard of care?

Why don't we hold companies to some kind of warranty?

It was fine when computers were just doing word processing, but when they are maintaining infrastructure, critical infrastructure, why is it that they don't have to give a warranty?

MR. PALLER: Don't you destroy the open source movement then? Because then there's nobody to sue.

MR. SCHWARTZ: No accountability.

MR. STANCO: No, I don't agree with that. What I was trying to say before is the government should make rules for everybody, then everybody rises and falls, and I think open source is going to do fine. It's a better model, in my opinion.

If it wasn't a better model, how could it possibly compete with billion-dollar companies when open source has no corporate structure, has no real structure except the Internet and a license, has no friends in high places, anyway, until recently, and still, it competes. Not only does it compete, the whole industry is going that way. In fact, it looks like UNIX is going to drop off and it's Microsoft versus open source -- or LINUX.

I'm not worried about how it will compete. My concern is I think we should have competition, I think we should have incentives as a set-up by the government. Then the government should really back off, and I think open source has to create its organization. It's still in the formative stage, but once it does, I think it should give warranties, because I think people should be held accountable.

How can you possibly build an infrastructure that everybody in the whole world depends upon, and these people just are basically saying, well, don't look to us. That doesn't make any sense.

And if we do that, if we set up the standard of care, I think what happens eventually is you have metrics that will play into that, and more importantly, you'll have an insurance industry that can come into play and then really enforce.

MR. SILVER: Kathy?

MS. BOHRER: I want to address your original question a little bit.

I think technology can do a lot to really put into place something that tries to meet requirements for appropriate use of data, as long as the data is in the system. Of course, there's always a limitation, because at some point, the data goes outside of the system. It's displayed to some person. It's printed out. Some person sees it and now knows it.

And at that point, if there's misuse outside of the system, then you need accountability because –

MR. SCHIAVONE: But is there an audit trail to that?

MS. BOHRER: You can have audit trails. In fact, I thought that if you turn around some prophecies -- and data minimization is part of that but not the only thing you can imagine.

If you actually automate more, you could actually protect privacy more, because you could eliminate humans dealing with personal data to a larger degree.

So, for example, if I place an order, my address goes into a system. No person sees it. When the box with my order comes along the manufacturing line, some label gets printed out, it gets put on that, and it gets shipped to me. No person ever saw my address.

That's just one example that occurred to me today as I was thinking about this, but it is interesting.

There are limits, but there's still a lot we could do a lot better than we are today.

MR. SILVER: Next question. Please keep them concise.

QUESTION: Yes.

There were a number of references today to best practices, and I am a great fan of having people follow best practices.

The trouble is, about four or five months ago, I was on a panel considering security technology for the health care industry, and two of the people on the panel were IT people from major health care providers, HMO's in California, as it turns out. I remember the debate I had with one of them, who wanted to know what are the best practices, and he capitalized the "B" and the "P", because from his point of view, HIPAA was the threat.

Attackers were not the threat. HIPAA was the threat. The danger to him was that his company would be sued. The danger to him personally was that he would be held responsible.

What he needed to know are the five simple things that he had to do called best practices such that, if he did these, then he was not legally responsible anymore.

So, if that's what we mean by best practices, I'm totally against it.

MR. NEUMANN: Ideally not. That's the lowest common denominator phenomenon, and that's clearly a disaster, but best practices themselves are useful. If you look at the generally accepted security principles that came out of our National Academy study from 1990, they're useful, but if they're not applied by people who know what the hell they're doing and who have a set of meaningful requirements in the first place and who have an architecture for the system that they're developing that is evolvable and inter-operable and so on, then the best practices are inherently not very useful.

So, it's much more than best practices.

MR. SILVER: Next question.

AUSTIN HILL: There's been a lot of discussion about the marketplace for technologies for protecting consumers’ information and I think, in the security area, we've had a long history of seeing this.

There's active threats, so it's a very easy, provable thing saying we're being threatened, so we need a firewall.

People got through the firewall, so now we need IDS, now we need patch management.

Companies can come in and say there's risk management, we have to spend so much to manage this risk of being attacked, and in the privacy side, if I look at the history of the privacy industry, which, I've been around a few years now, I haven't seen that evolve. A few years ago the FTC started announcing they were doing a great initiative, checking websites for policies. So, everyone threw up a policy.

All of a sudden you should have a CPO.

So, a whole bunch of CPO's were named, but generally they were lobbyists, to make sure no more privacy laws were assigned.

If you actually talk to CPO's about what's your budget, how many IT projects have you initiated, have you changed your database handling, it’s non-existent.

Same thing in Europe. This is by no means only a problem here.

Even in Europe, where legislation was passed and there was heavier legislation, without some enforcement or oversight into what companies actually are doing to change their practices, how they handle data -- that didn't exist until recently when we've seen it start happening. In the Netherlands, they've started doing spot checks on companies and reviewing their data handling practices, and in the last six months, we got more inquiries from the Netherlands than I have had from the United States for privacy management products.

When I start to look at the evolution of a marketplace, what exists to try and create that? We've seen safety belts, air bags. Those markets evolved because there were some standards set, there was some liability standard or regulation that said you have to be at least this safe, either through civil litigation or some other mechanism.

I just don't see that happening at all in privacy. So, generally, it becomes let's just put our head in the sand, put up a privacy web-page and hope no one calls or comes looking.

MR. NEUMANN: Austin, even though your question is very different from Carl's, my answer is exactly the same. It requires a great deal more than this litany of simplistic non-solutions.

It's a holistic problem. It requires an end-to-end solution.

It requires an understanding of architectures, software engineering, of having requirements that are meaningful in the first place, of submitting to some sort of evaluation process, of submitting to open review, perhaps, or at least having teams beating the hell out of your system, of understanding the privacy requirements before you go into building the system in the first place. There are no easy answers.

If you look on my website, you'll see lots of reports on how to build systems properly.

Nobody pays any attention to them, as far as I can make out.

MR. SILVER: I would add that the FTC Safeguards Rule went into effect recently, so please stay tuned.

And the last question, please.

QUESTION: Thank you for indulging me. I hope it's worth it.

Alan Wilcox. I work for the Vanguard Group.

I'd like to mention, also, that we don't have a CPO. We don't even have a CISO, because that spells N-o-t-h-i-n-g.

The regulations require a mature information security program, and that's what our goal is, to have a mature program.

I've got a comment and then a question.

Several comments have been raised that seem disparaging of overseas development. It's exactly the same criticism of foreign cars, when foreign cars were first being made. The issue is, if they can write code better than the processes and programs that we have in place, I welcome overseas development, if they have better checks and balances, if they have a more mature product development cycle.

Ultimately, American cars got a lot better, because we had a lot of Hondas and Toyotas around, and now we have a lot better GM's, Fords, and Chryslers. I think the same thing might bear out with overseas development.

Also, if you don't think foreign nationals are already writing a lot of your software, you haven't been to a lot of software conferences.

I won't try to do my Indian accent impersonation.

Finally, how applications are being used is often completely left out of vendors' equations. Within my company, we see a lot of vendors saying, well, yes, here's a great database application. It has to run with elevated privileges. It has to run as the root user on your system.

Well, that's bogus. That's a practice that absolutely must not be tolerated.

Vendors should not have the ability to dictate the security environment of the customers. It goes the other way around.

Thanks.

MR. NEUMANN: That was a question. Very good question, actually.

MR. SILVER: Howard, go ahead.

MR. SCHMIDT: Just one really, really quick comment, and that's in reference to the comment on foreign nationals writing code.

The most severe intelligence threats against this country have been by born-and-bred U.S. citizens such as the FBI guy and Aldridge Ames and company, and this has been an issue that pops up from time to time.

We have got phenomenal foreign nationals writing code, doing trustworthy things, doing good work. So, I wouldn't look at where they come from but look at the product they're putting out and the quality control and the engineering that goes into it.

MR. PURCELL: I would also comment on who writes code.

There may be an advantage to a less mature software industry emerging from another national sphere or geographic sphere. One thing that you might have heard today is that it may be the maturity of the process that's our biggest problem to overcome -- the Windows code bases, 10 million lines, 50 million lines, I don't know, some extraordinarily huge number of lines of code, which has been patched and cobbled together over a long, long period of time. It may be that one of the reasons that open source works well today competitively is because it doesn't have that maturity, because it is starting over again.

One thing that we don't do -- and nobody should ever think that this is happening -- is for most software that you're using, you don't sit down and write new requirements and write new software.

It's an adaptation of what's been written before. The requirements are simply, okay, it didn't do this very well before, so make it do this now. So, it's re-jiggered for that, and then here's some new stuff it can do. It's kind of like your '57 Chevy spiffed up. So, I would be very careful to say that it may be the maturity of our industry that's something we have to overcome in many ways.

MR. NEUMANN: I would like to bring the foreign national argument back to my electronic voting machine. Suppose that the software and the systems were built by, say, the Russian mafia or the Bin Laden Research Institute. I think you would be very concerned about using those systems in your elections.

MR. PURCELL: No question. I would be very concerned.

But I would bet that, if they were built from scratch, that they worked very well according to the interests of the builder, right? And that is what I'm saying.

I'm not saying who should or should not build our code. What I am saying is very little of domestic code is actually being built from scratch.

MR. NEUMANN: My comment is also that you would never find the Trojan horses that they put in there.

MR. PURCELL: Right. I agree.

MR. SILVER: Well, it's getting to be about 5:30. How about a hand for our panelists?

(Applause.)

MR. SILVER: I also want to introduce my boss, who is here with some closing remarks. He's the director of the Division of Financial Practices, Joel Winston.

(Applause.)

CLOSING REMARKS

MR. WINSTON: I guess I get the final words, and I want to thank all of you hardy souls for sticking out the day. You're rewarded by having stayed here all day, now you get to go outside when it's not raining. So, congratulations.

I want to thank the panelists and the FTC staff for their thoughtful work and enlightening discussion today. This workshop had a different focus than the one last month, but in many respects, the lessons are the same -- that security technologies need to be easy to use, compatible with other systems, and applications, and built into the basic hardware and software consumers and businesses use.

In addition, the two workshops together have raised larger themes of how people, in general, can better use technology to protect sensitive information, whether they're engaging in commercial transactions or simply carrying out their everyday affairs.

The day began with the release of a report showing how businesses are currently addressing privacy issues, including the security of information they collect. It showed that businesses still have some work to do in this area, work that could be helped along by appropriate and accessible technological tools.

We then saw an impressive display of improvisational skill as panelists discussed a hypothetical illustrating how a medium-sized business can take advantage of the Internet while at the same time addressing privacy concerns.

The panelists collaborated to develop a risk management plan to help make information and systems safer.

We also heard about the wide array of technological tools available to help businesses protect personal information, including, for example, one that can digitize a business' privacy policy to allow automated monitoring of data flows consistent with the policy.

Panelists addressed the issues these technologies raise for businesses, including out-sourcing issues for smaller businesses and the consequences of poor inter-operability between different architectures and vocabularies.

In addition, we learned about the various legal standards and industry frameworks that have arisen in recent years, efforts to expand their use and the obstacles faced in implementing them.

Panelists also discussed marketplace incentives for privacy improvements such as offering discounts or adjusting contractual obligations.

While still not the norm, use of these incentives is increasing rapidly.

Our final panel addressed the critical question of how to design business technologies so that they include built-in protections for consumer information. As at our last workshop, panelists were critical of the approach that has dominated the field thus far, which is to purchase add-on products or issue patches, sometimes hundreds of them, as problems arise.

Although the challenges are considerable, we heard about several promising approaches toward building a culture of security.

For example, at least one computer manufacturer is shipping systems that are configured to meet benchmarks defined by the Center for Internet Security.

As we heard, people, policies, and technologies are all three necessary ingredients for a culture of security.

The panelists also took up the debate about the merits of open source versus proprietary technologies. In the end, they agreed that no matter where the code came from, the key ingredients for secure systems are sound practices and rigorous quality control.

As to whether open source or proprietary software more often meets these goals, I think I'll leave that to the test of time and future discussions.

Clearly, this is all an organic process. Virtually every day, new security concerns arise, and new technologies for addressing them are developed. There are no magic answers here, no easy solutions, but it's critical to keep the dialogue going and the information flowing.

It's an old saying -- I think it was originally Thomas Edison who said that genius is 10 percent inspiration and 90 percent perspiration. I think that's a good formula for what we need here, some creative thinking and lots and lots of hard work.

So, let me thank everyone again for coming. Discussions like these demonstrate that talented and dedicated minds are trying hard to find solutions to a leading challenge of our information age, harnessing technology to help consumers and businesses provide better protection for consumer information.

I wish you all good fortune in this very important endeavor.

Thank you.

(Applause.)

(Whereupon, at 5:32 p.m., the workshop was concluded.)

* * * * *

CERTIFICATION OF REPORTER

DOCKET/FILE NUMBER: P022106

CASE TITLE: HEALTH CARE AND COMPETITION LAW AND POLICY

DATE: JUNE 4, 2003

I HEREBY CERTIFY that the transcript contained herein is a full and accurate transcript of the tapes transcribed by me on the above cause before the FEDERAL TRADE COMMISSION to the best of my knowledge and belief.

DATED: JUNE 11, 2003

ANDREW N. SCHACHTER

CERTIFICATION OF PROOFREADER

I HEREBY CERTIFY that I proofread the transcript for accuracy in spelling, hyphenation, punctuation and format.

SARA J. VANCE