FEDERAL TRADE COMMISSION

I N D E X

FEDERAL TRADE COMMISSION

IN RE:	)	
PROTECTING CONSUMERS IN THE	)	Matter No.
NEXT TECH-ADE	)	P064101
----------	)	

WEDNESDAY, NOVEMBER 8, 2006

GEORGE WASHINGTON UNIVERSITY
LISNER AUDITORIUM
730 21st Street, N.W.
Washington, D.C.

The above-entitled workshop commenced, pursuant to notice, at 9:00 a.m., reported by Brenda Smonskey.

P R O C E E D I N G S

- - - - -

MR. BURG: Good morning, and welcome to the third day of protecting consumers in the next Tech-ade.

I hope the election last night hasn't taken too much of a toll on you.

This panel this morning is about changes in payment devices and systems.

We are going to be looking at a number of technologies and systems that will echo some of the technological advances that we have heard about over the past couple of days. You will hear about contactless credit cards, biometric payment systems, the use of cell phones to make payments.

I'm Elliot Burg from the Vermont Attorney General's office. And from a consumer protection or law enforcement perspective, I think the point at which consumers pay for goods and services is a critical juncture with respect to consumer education, with respect to consumer rights and with respect to law enforcement.

We have a large and wonderful panel this morning. And these folks are going to be telling you about the devices and systems that are emerging, and

some of them are in full use in other parts of the world at this point or in the United States.

There will be a discussion of opportunities and issues of fraud and privacy related to these payment devices and systems, and there will be some discussion of potential solutions to issues of fraud and privacy.

I will introduce members of the panel as they present today. I would appreciate it if you would just hold your applause until the end of the entire panel.

One of our panel members, Tom Keithley from I4 Commerce, is not here today, but we have a couple people that will at least informally try to fill in for him.

We will divide this panel into three parts. The first part is an overview, focusing in particular on electronic payment systems.

I would like to introduce Dr. Jeanne Hogarth from the Federal Reserve Board.

MS. HOGARTH: Great. Thank you. I'm a former college professor. So I will go over to the podium because professors like to lean on stuff.

Do I advance this to get me started? It will come up.

Okay. About a year ago, the Fed conducted focus groups on payroll cards, one of those payment technologies for people who choose not to have a bank account or have their paycheck direct deposited into a bank account.

When we talked to consumers, we got a range on how consumers use these cards. One person said I strictly just get my entire amount of whatever has been credited to my account out and cashed. So the card is a basically an ATM card for that person.

Another person said I use it just like a checking account, I leave my money in there and I use it as I need to.

And a third person said when they used to give us a check, I would be broke, I have some money now from payday to payday. So they saw this as a real financial management tool to help them.

If you think about it, when you cash a check, that money is in your wallet with little voices saying "spend me, spend me." This was a way for him or her -- I can't remember which -- to manage their funds.

I need to issue a disclaimer that what you are hearing today from me is just me. It does not represent the views of the Federal Reserve Board, the

Board of Governors or the reserve banks or any of the staff. It is just Jeanne.

So let's talk about what changes in payment streams have been happening over the last few years. And our data, this data comes from a Federal Reserve bulletin article that you can access on the Web.

It basically shows you that in 2000, checks amounted for 58 percent of the number of transactions and 66 percent of the dollar value of those transactions.

By 2003, that had come down to only about 45 percent of those number of transactions and about 60 percent and some change of the dollar value of those transactions.

Credit cards rose a little bit, from 22 to 23 percent of the number of transactions. Debit cards really took on a lot of that gap, moving from 11 percent of transactions in 2000 to 19 percent in 2003.

And ACH, which I know you have heard of and you will hear more about this morning, went from 8 percent of transactions to 11 percent of transactions and from 31 percent of the dollar volume to 37 percent of the dollar volume.

I think it is interesting to note here what

we don't know about those transactions are where are the small ticket items and where are the big ticket items, when consumers have to spend five, 10 bucks, how are they spending it, and when I pay my mortgage, how am I paying my mortgage.

The big dollar items versus the small dollar volumes are sort of an interesting thing.

When we look at how do consumers use technology, this happens to be from two different data sets. The 2001 and 2004 data points are from the Federal Reserve Board survey of consumer finances. The 2003 data point is from a survey that we used with the University of Michigan.

So there are slightly different samples. So a lot of difference you see between 2003 and 2004 is really a vestige of the sampling framework and not of the actual trending, I would say.

But you can see nonetheless that more people are using ATMs, a slight dip in direct deposit. More people are using strong banking. Certainly more people are using debit cards.

More people are using auto paying. And automatic bill paying is I tell my bank on the 15th of the month, always pay my car payment, on the 15th of the month, always pay my rent or pay my mortgage.

That's different from going online and arranging for the payment to be sent to my credit card company, to the cable company. That would be done by PC banking which, again, you can see a big rise in PC banking, from about a fifth of consumers to about a third of consumers.

When we look at technologies, we often think about the old technologies that people use, ATMs, direct deposit, phone banking, automated bill paying.

Even here these old technologies are changing. ATMs are going a lot more into market segmentation. We have ATMs that are owned by banks and ATMs owned by what the industry calls ISO, independent sales organizations. Those are the ATMs you might see in a convenience store or in a gambling casino, let's say.

Interestingly, the deployment of new ATMs has outpaced the growth in the number of users. What we are seeing is fewer transactions per ATM that on the surface you might think, well, lower revenue per ATM, so eventually we will hit an equilibrium.

The reality is that a lot of the growth in ATMs is coming in what we call foreign ATMs. These are ATMs where they can charge or surcharge a user fee. Not only would your bank charge for using that,

but the ATM itself charges. We are seeing surcharges going up all the time.

Other new trends that we are seeing in ATMs, imaging, so you will soon be able to scroll a check into the ATM and have it act as a check casher, assuming you have an account with the bank.

There are a lot of new technologies emerging with the ATM. There it is.

We have already seen in the data fewer checks, more debits. Debits allow faster processing at point of sale, the lines are shorter and people can get through more. None of us likes to wait in line too long.

Two-thirds of adults have purchased or received a gift card. 55 of those spend more than the initial value. You can see why retailers like gift cards.

In 2005, 90 percent of people used some sort of plastic credit cards, debit cards or prepaid cards. That's up from 78 percent in 2000. We are also seeing things like consumers write a check to pay their utility bill but that check is processed as a debit. It is electronically converted.

I have mentioned payroll cards, mentioned prepaid cards, and we all know about credit cards.

Consumers really do have a choice of paper, plastic or electrons.

There are even more electrons out there in the marketplace. Those of you who are in the Washington area obviously know about the SmartTrip cards.

We have seen a rise in online banking. You saw the data from a fifth to a third of people using PC banking. We have seen in Internet transactions the evolution of PayPal, in addition to using debit and credit cards.

We will be talking later this morning about the contactless devices, the radio frequency devices, the contactless debit and credit cards, the speed pass, the EZ Pass that many of us use in and around the highways in the Northeast area here.

We are going to be talking a little bit about reloadable versus single load. I think one of the issues that we all want to sort of keep a handle on for this group is what are the consumer regulation implications for a reloadable card that might be different from a single-load card.

So when I get the gift card from the bookstore and I'm not going to reload money on it, maybe I need a different set of consumer protections

than when I have a reloadable card that I might lose and I might have a substantial amount of money on it. I hate to tell you how much money is on my SmartTrip card right now because you will all mug me leaving the stage.

There are issues of seniorage and unclaimed funds and who gets those moneys and if it's the state in which the card was sold, the state in which the company is headquartered.

There are some interesting issues out there with respect to unclaimed funds.

We did a survey a number of years ago and we looked at how consumers break out in their use of these products. We found five basic clusters.

Big surprise, there are people who don't use them at all, and those tend to be low income, elderly, less educated, no surprise. The mega users, the people who use everything are exactly the opposite side of the scale, the high income, high education, younger people.

The people who are using the EZ pays, the phone and PC banking and auto payments, tend to be the highest income and best educated. They are also us middle agers. Interesting thing to think about.

Okay. Challenges and opportunities. There

are pluses and minuses to all these technologies. Part of me as a consumer educator says I see the real advantage in helping people improve their financial management. You don't have to go to the check casher, cash out your whole check and walk out of there with a giant "rob me" sign on you.

Like that first quote I read you, it helps me manage my paycheck so I have money at the end of the month. There is a lot of real good potential for these products.

There is always the dark side. We will talk more about the issue of fraud, identity theft and issues like that. There are technology gaps not only between the haves and the have nots, and I think that kind of gap is narrowing. There are also with the clustering issue issues of income and age.

And one of the issues becomes are we really going to just age out of this problem or are we going to have the problems change.

So with that in mind, I'm going to turn this back over to the next speaker and we will move on from there.

Thank you.

(Applause.)

MR. BURG: Thank you, Jeanne.

We are going to have a brief international perspective here by video. Delia Rickard is a regional commissioner for the Australian Securities and Investments Commission. I understand we are going to roll her presentation now.

(Whereupon, the video was played.)

MR. BURG: We had bit of an echo up here.

I will turn to some of my respondents. I would like you to focus on Jeanne Hogarth's presentation and particularly with respect to what I would call the more traditional forms of electronic payments that are out there, maybe increasing in use.

Our discussants are Jean Ann Fox from the Consumer Federation of America and Paul Tomasofsky from Two Sparrows Consulting.

Your thoughts on Jeanne's presentation?

MS. FOX: Thank you very much. Good morning.

Consumers need to have confidence in the payment mechanisms that they use. That is generally provided by enforceable consumer protection law.

What we have seen in the payments marketplace is an explosion in the different types of plastic that is available to help consumers spend their money.

But the consumer protections have not kept up

with the plastic proliferation. So you have one set of rights if you use your credit card, another set of rights if you use a debit card. You have absolutely no federal consumer protections at all if you use a stored value card or prepaid debit card, as Jeanne described.

Starting next year, if you are paid by a payroll card, the Federal Reserve has said that you will be protected under the Electronic Funds Transfer Act. But the cards that are being provided, especially to low-income consumers, unbanked consumers to function as a bank account in your pocket are not protected by any federal law.

As a transAtlantic consumer dialogue advised both the U.S. and the European Union a few years ago, we need to harmonize consumer protections so that they apply to all forms of payment mechanisms so consumers can be assured that there are liability limits if your card malfunctions, there is recourse so you can get your money back, there is a dispute process, so there are billing standards if a bill is involved.

We think there should be some simple principles that apply to protecting consumers regardless of the type of payment mechanism that you

are using. The protection should be universal.

They should apply to every form of payment mechanism. They should be uniform to the extent possible. Right now, if you write a check, it can be processed in one of several different ways and each way involves a different set of protections. It is completely confusing to consumers.

The third principle for protecting consumers in the payment market is that there shouldn't be any reduction in protections that consumers already have. For example, we are all used to the $50 liability limit for unauthorized use of a credit card. That would make a good standard regardless of the type of card involved.

MR. BURG: Great. Paul Tomasofsky.

MR. TOMASOFSKY: I think as we talk about new and evolving forms of payment, I like to look at the business models, the business models from the providers as well as the consumers.

What is the compelling business case to be able to make these products work in the marketplace? There are a lot of products that have been tried over the last 15 to 20 years, even as me move to more and more electronic. Most of them have failed.

So we look for what's the business model and

what is the compelling argument, why are consumers going to use it. Consumers are demanding convenience, more and more convenience in their products today. Electronics provide that.

And also one of confidence. We mentioned confidence already. I looked at confidence from a different angle, from that of fraud or confidence that the system, that the product can be used and someone is not going to take your money.

We hear a lot in the press about ID theft and about takeover of accounts, et cetera. Consumers are starting to wonder is it safe to use my credit card.

In fact, empirically we know that some consumers have taken out different cards, a new credit card or debit card, specifically for Internet transactions and they segregate their payments because they want to put a human firewall around what happens there. Those are the kind of things that as we are developing products in the industry that we need to keep an eye out for.

MR. BURG: Thank you. Just to underscore Jeanne's point about the nonuser group, there is a recent report from Larosa that talks about the high cost of remittances from the United States to countries in Latin America.

And I think the underlying reason for that that's flagged in the report is many people who send remittances to Latin American countries don't have a bank account. There is a group of Americans, even before we get to things like contactless credit cards, who are not even plugged into the banking system.

I would like to turn a little bit future now with the second part of the program. We are going to talk about new payment methods now, state of the art and predictions. And I think we have a short video on near-field communication.

(Whereupon, the video was played.)

MR. BURG: So here to talk to us in person about NFC technology and contactless payments is Mark MacCarthy from Visa USA. Mark.

MR. MACCARTHY: I'm going to wait for that device to load. I have been told to be patient, it will get there.

Thanks very much. I do want to say a couple things about some of the issues that were brought up earlier, and then I will get into the discussion on contactless payments.

Just responding in no particular order to the comments that were made, this is the agenda for what

we are going to be talking about.

Jeanne and I have talked in a large number of instances about this issue of consumer protections. And there are different legal standards for consumer protections between debit and credit cards and some payment systems, mobile payment systems, where the carrier does the billing, third-party billing having no legal consumer protections at all.

She has been proposing for years this idea of a harmonized operation. We don't think it is a crazy idea. It is an idea worth pursuing.

At some point the marketplace may need to be constrained with a uniform floor that applies to all payment systems so consumers have a sense of what their fundamental basic protections are and competition can work above that to provide additional consumer protections.

That's the way it has worked so far. Visa has equalized consumer protections across all its card products so we have zero liability for debit, credit and prepaid. We have identical refund rights and dispute resolution rights for all the different card products we have.

An effort that would harmonize legislation in this area probably would be something worth

exploring. On the fraud point, we will be talking a little bit about this in the context of the contactless operation.

It is important to remember that the Visa cards and Mastercards and the American Express cards are very safe products to use, our fraud rate is low. It is 6, 7 cents for every hundred dollars worth of fraud. It has been on a downward trend for a couple of decades due to the investments we have made in neural networks and other fraud detection devices.

One of the newest ones we have is called Advanced Authorization, where at the time of the transaction, a risk score is calculated and provided to the issuing bank so the issuing bank knows the likelihood that transaction might be fraudulent and it includes information that has to do with whether or not the card number had been involved in a data breach.

It is the kind of technology that we think will help to improve our ability to catch fraud and prevent it before it even happens.

So where are we going in this contactless demonstration? I have also been told to be patient when you push the button, that it will move if you push it and you shouldn't push it twice.

This is the opportunity for us in the contactless area. Our enemy in this area is cash and checks, in particular cash.

If you look at the numbers here, we have a possible marketplace of $1.2 trillion to go after with our contactless operation.

I do want to say that the numbers that you heard about earlier from the Federal Reserve are reflected in Visa's numbers. Our debit card transactions now exceed our credit card transactions.

In 2005, debit represented 43 percent of the sales volume but represented 63 percent of our total number of transactions.

We find that debit cards are being used for everyday transactions. We have also noticed that in terms of the discussion here of the role of electronic payments -- Jeanne didn't mention this -- electronic payments, as you can see from this chart, have passed cash and checks as the majority form of payment in the United States.

The prepaid card operation, it is a nascent market. We don't want to exaggerate the size of it yet. It is a $25 billion business right now, which is compared to the total sales for Visa of 16 percent of personal consumption expenditures.

And I just want to emphasize before I leave that Visa protections apply to all of those products.

All right. Contactless. Why do people want contactless? There are three different groups of people who would be interested. One is the consumers themselves, the issuing banks who would want to issue the cards and the merchants who want to accept it.

For consumers, it is fast, it is convenient. You saw the reaction from some of the people at the test there in Atlanta. It is cool. It is a bright new technology that people would like to use. For merchants, it is speed at check-out, shorter check-out lines.

They will be doing their cueing theory analysis to find out whether they are getting enough benefit to make it worth the investment.

For the issuers, they get extra volume, extra use of the card, they get loyalty for people who like the kind of operation they have, and they are looking forward to differentiation.

The contactless payment features that I want to show you here, the ones that had to do with the use of the card, not through a cell phone but through a card itself, you want to make sure that the technology is usable to insert card payment

information into our payment network. It is not designed to be part of any kind of ubiquitous RFID network.

We want faster and more convenient ways of getting information into our network. This is what it looks like at the point of sale if you go to CVS or McDonald's. This is the kind of technology you will see.

It is important to notice that Visa and MasterCard have harmonized the standards involved here. The communication between the card and the reader has been standardized to make it easier for the reader to be produced.

The evolution of contactless, you saw where it was going by seeing the near-field commercial.

There are two directions it goes in. One is into mobile phones. Because there is a chip on the card, it also goes in the direction of smart cards.

The contactless penetration is pretty good. There are 6 million Visa cards globally. We have three different issuers doing it in the United States. And Mastercard and American Express are also in the marketplace.

Let me move on here, if I could.

These are some of the merchants who are using

it. We have 7-Eleven, CVS, McDonald's in this area and there are others nationwide. We have contactless in about 30,000 locations in the United States, and that's growing.

MR. BURG: We are getting a time out signal from our relentless timekeepers.

MR. MACCARTHY: I am actually finished. I am happy to wait for the controversial questions about the security of this until we get to the end of the discussion.

We think it is a good technology. It is growing. We are hoping to fill in all those states so it looks more like the Democratic victory last night.

MR. BURG: Thank you.

The second form of payment device in our trilogy this morning is a set of alternative payment types, including PayPal, phone operator based billing and Microsoft points.

Here is David Turner from Microsoft.

MR. TURNER: I don't have a deck to go through. In talking about alternative payment types, I really want to emphasize a point of view that what we are moving towards is a separation, actually not moving towards. But what we are learning to

understand is that there is a separation from the identity user making a payment and the mechanism by which you make the payment.

If you think of your credit card today, the regular old piece of plastic you have and I will even go to far as to say it is contactless, you already have five different ways of transferring that identity to make a purchase transaction.

You can give it verbally, you can have it imprinted, swiped, there is contactless and then there is self-entry, if you are doing it on a laptop or computer into a Web browser.

You already have five different ways of taking the same payment information or payment identity and executing a transaction.

What we are finding is happening, though, is other forms of payment mechanisms are coming into play and have been for quite a few years to try and solve various convenience issues and to solve certain usage scenarios that existing systems don't currently support.

Peer-to-peer currency exchange is one that people can't do today. PayPal allows you to do that over the Web and, of course, is becoming quite large as a result of things like eBay.

There is no way I could do an electronic currency exchange with Mark just by tapping our phones together.

With technologies like NFC being available, we have the technology that would allow us to make an electronic exchange of some sort. We don't have the backend fulfillment to solve the rest of the problem.

The main thing I really want to emphasize is that as we move forward, I think what we need to think more and more about is the distinctions between the payment identity that you have and you use and the protection and services you get from that payment identity from the mechanisms that we use to apply that payment identity in a variety of different scenarios.

So, of course, that means different people are trying to get into the business of being the payment house. I'm sure Mark will agree. There is a fair amount of money to be made in this business.

Cell phone operators have a unique opportunity in that they have already got a secure representation in every handset that's out there, and an identity that is at the same level of trust as I would say the rest of the credit card companies have with the consumer.

What they don't have yet, of course, is the same backend dispute resolution and -- I forget all the proper terms -- actually paying the vendors who actually sold the products.

There are a lot of backend services they don't tie into yet, which is the challenge they are trying to address.

As far as trusting the consumer, as far as security goes and their ability to fulfill just the consumer-level payment, they are in a very good position for doing things like micro payments.

You think of your current cell phone bill today -- certainly mine -- I get this long, very long list of atomic transactions, every single time I did anything on my device, whether it was check voice mail, send a text message, go online for data, answer the phone, whatever it happens to be. I have a record of that.

That's micro billing. They are keeping track of my data usage even though I have a bulk plan, even though somewhere in the -- it is less than a kilobyte per use is the level at which they are tracking.

So they have a great system in place for doing micropayments. But again, that's sort of the rest of the system that is not in place. They don't

have a relationship set up with banks and vendors and with other people. That is one of the challenges that they have.

The reason that Microsoft, of course, is interested in all this is as these systems move forward, our goal is to help provide software that enables the exchange in a secure, trusted way of those payment identities regardless of how you choose to do it, whether you enter it in a browser and then it connects to a backend server, whether it is through an NFC payment, through a card or one of the things Microsoft is actively involved in, which is the NFC forum, having it integrated into a mobile device so you can use it at point of payment.

We want to be able to make it so that all of these transactions can work very much in a way that Jean Ann was talking about, where you don't have to think about which identity or which payment mechanism am I using in which scenario.

If you choose to pay by Visa, it is your Visa identity that is used, and you get all the value and benefits from Visa or, who knows, maybe a cell phone provider in some circumstances.

There is a lot of new systems coming on the market. Some of them do well.

Paul pointed out earlier we have been trying for ages, many of them trying to address some convenience and situations that we can't really accommodate yet.

But in the end, I think what it is really going to come down to is falling back to the same sorts of trust mechanisms that we have in place today.

Just as a quick aside, an interesting discussion yesterday about advertising, and the woman from Acxiom pointed out that she has been in the business for 30 years and, quite frankly, targeted advertising hasn't changed.

Technology has changed. The data level of details have changed, but targeted ads haven't. Sears as a catalogue store became huge because of the trust they provided and the service that they provided, no-question returns.

The credit card companies, Mastercard, Visa, Amex and so on, they have gained the trust of their customers. That's a huge added value regardless of the technology being used.

MR. BURG: We have one more presentation from devices and systems from James Linlor, Black Lab Mobile, a focus on mobile phones.

MR. LINLOR: Good morning.

I would like to talk about a couple of details that we have right now. You will see from the slides -- this is actually going to be a drinking from the fire hose presentation so we go through this quickly.

Right now there are a number of billing systems that are available as far as carrier billing, and what David mentioned as far as micro payments, we are actually looking at what we call minipayments, which is the range between $2 and $200 primarily, and it also can extend beyond that.

As far as consumer protections, there does need to be some type of uniform standard, as Jean Ann was mentioning before.

Right now what cell phones are primarily being used for as far as payment systems is a lot for ring tones, and some content. There is really no hard goods or tangibles that are being purchased through cell phones.

What we developed with Bill My Cell and Black Lab Mobile is to be able to work on existing cell phones. Right now there are over 200 million cell phones. You saw the presentation with Philips.

That's a great idea, but also it would be

nice and what we have developed is to be able to use your existing cell phone. Wouldn't it be nice to use the phone that you have today to be able to pay for a parking meter, pay for a pizza, buy a movie ticket, get a concert ticket, be able to do all these things with the device that you have right now.

There are systems right now that are set up and in place for this. That's I guess one of the things I want people to take away from this series of presentations, is that while the consumer protection is certainly key to this moving forward, that's one we all have to address, the point David made about being able to transfer money person to person, that can be done today using your existing cell phone today.

It cannot be done easily in a contactless RFID format, but it can be done using SMS and other technologies.

So looking at what we have in place today, there are money transfers, both consumer to consumer and consumer to business. This is in place, it has been around for a couple of years already. The idea of being able to pay for a taxi by calling a phone or sending a text message, and transfer the money to the driver so that their phone shows they received the

payment in a trusted fashion, you get a receipt back on your cell phone, and you can print it off from the Web later on.

It is a great system. It requires adoption and trust. This is part of what Visa went through when the Visa card and Mastercards were being rolled out initially.

It will take time for people to actually be able to have that level of trust.

Looking at systems and threats, you should understand the way the systems actually work. There are actually a number of providers, and Bill My Cell and Black Lab Mobile are one of them, and they use what are called short codes. It is an authentication system to be able to use the wireless networks.

You use a short code, sometimes an IP address and different types of passwords and others, some mall security methods, to be able to access the wireless network. That in and of itself is now secure.

As I mentioned on the slide, there is a false sense of security. They can be hacked. At the same time, those hacks can be guarded against.

As the wireless networks are being used more and more for payments and consumer convenience, the

wireless carriers also have to step up to the plate and be part of the solution to lock down their networks. And that is not the situation today.

Looking at mobile payments and systems of what's going to be coming up, there will be more mobile transactions, more RFID transactions, and RFID and near-field communications will be part of the solution.

It is great to see the market looking at how can Visa and Mastercard be rolled out further across the country. The issue becomes point of sale integration. It involves the readers that we are talking about and the cards we are talking about, matching those up so you actually have the card out there or, in the case of that Philips presentation, showing you can swipe your cell phone.

If you look at how many cell phones right now are out there and how many readers are out there and how often do the two come together, it is not a lot.

If you can use your existing cell phone -- and that has been our approach -- it is a whole lot more. What can we do today, I will move on, because you can see on the slide a picture of a car and a parking payment that you can pay for airport parking right now, again, using your cell phone. So you

don't need cash to help you find your car later on.

Part of this all ties back also to location sensitive and location awareness. And if you have the location awareness, you can do a lot of great things with security, and you are going to be able to provide a lot more consumer benefit by being able to have also different types of advertising, different types of information.

The last slide here is looking at some threats. The biggest issue that I see as far as looking at mobile payments and mobile information and even moving into biometrics -- we will be talking more about that today -- is what information is stored where.

Right now you have a cell phone, as David was mentioning, and the wireless companies are doing a great job of tracking all this. But it will become a honey pot. Just like right now your credit card gets taken, that becomes a honey pot.

In the future, as biometrics are going to be stored, how that is going to be stored will become a big consumer issue, to make sure that information doesn't become a honey pot also.

MR. BURG: That's a good segue to an issue I would like to mix up a little bit here, the pervasive

issue of security.

Some of you may have seen the article in The New York Times recently on this RSA Labs experiment that was done which involved reading information from a contactless credit card through an envelope, and it conjured up the specter of people walking through Times Square with a small device and basically harvesting information.

I know Mark MacCarthy from Visa didn't have an opportunity to lay out his security slide. I wanted to see if he could have a go at it from that side and if the discussants and others for the next minute or so could have a go at it from the "we have to be very careful" side.

MR. MACCARTHY: The first point is that Visa has taken enormous steps to build security into our contactless product. Mastercard has done it too. So has American Express.

The reason is simple. The financial incentives are set up so that if we don't do security right, the product won't succeed. If there is fraud using this product and consumers perceive it in a widespread fashion as unsafe, they don't have to use it.

If they don't use it, the issuers won't want

to put it out into the market, and the merchants won't want to have it because there aren't enough users to make it worthwhile.

This is the kind of thing where the financial incentives seem to be aligned properly. The fraud losses, after all, if they do take place are not borne by the consumer. They are borne by the issuer.

If they are too large, the issuer doesn't have to issue the product. It will not succeed in the marketplace.

Because of that, we have put in place we think the kind of security protections and safeguards that are reasonably designed to protect against realistic risks of fraud in this area.

So we do have encryption. There is 128-bit encryption, triple encryption. There is a counter in the card and a way of calculating a special code that has to be transmitted through the system every single time. It is a different code every single time calculated by the processor on the card.

If the information is intercepted in the course of a transaction, it is not information that can be reused for another contactless transaction. It can't be used to manufacture a separate card.

In terms of the risks that were pointed out

in the study, there are a number of best practices that are building up in the area.

First of all, the issuers who are sending out the cards, the best practice is for them to send it out in a shielded fashion so it can't be read. The name of the person that is on the card itself need not be transmitted as part of the transaction to make it work.

So the best practice is for that not to be transmitted. So at the end of the day, if there is fraud in this area, there is zero liability.

We think that protects people. We have an ongoing monitoring program. We are looking at the levels of fraud in this area. We are comparing it to the overall level of fraud which I said earlier is around 6 cents for every hundred bucks.

If we suddenly see that in the contactless world it is 7, 8, 10, 20 bases points, that is clear something is going on.

We have yet to see fraud practiced in this area as a result of one of the hacks described in the press. We don't think those are realistic threats that need to be addressed at this point.

But it is an issue that we are monitoring, we are looking at it very carefully, and we are prepared

to make adjustments as we go forward if the marketplace requires it.

MR. BURG: I would like to see if we have an opposing or at least different view on the panel.

Let me flag the fact that we are looking at an array of payment mechanisms. It may well be, in fact, it is the case in the credit card area that the issuers or the companies behind them are bearing the risk of an unauthorized transaction. That's part of what the merchant fees support.

If you move over to RFID technology using cell phones, if I have an unauthorized billing on my phone bill for goods that I didn't purchase but somebody was able to sniff out the information and use it to make a purchase, where will I be left?

MR. MACCARTHY: If the payment mechanism you are using in that context is a Visa card and what is transmitted is Visa information and it goes through the Visa network, you have full consumer protections.

If it is a transaction that is provided by the mobile carrier itself, you have no protections.

I have had personal experience of trying to work with a mobile carrier to get some redress when my kid was in a download situation.

The mobile carriers do not provide redress.

If you have a problem with a ring tone provider, they will not solve it for you.

I will guess that James is going to have something to say about that. But I wanted to turn to our discussants.

MR. TOMASOFSKY: This is fun. I get to decide whether I want to pick on Visa or Microsoft. You usually don't get that opportunity in one room. I think I am going to do Microsoft.

Dave, you mentioned security and Microsoft working on security products. And this might be a low ball, but I have to tell you the marketplace, the perception is that Microsoft and security aren't necessarily sort of hand in glove, in particular, with your operating system and your Explorer.

I guess we have Vista coming out. We will see what happens there. The perception and the reality I guess is the question. How does a company like Microsoft, who wants to get into more and more of this type of evolving payments, how does it deal with the perception versus the reality?

MR. BURG: Let me see if we have a thought with Jean Ann, and then we will have the Fortune 500 on this side.

MS. FOX: Consumers have a lot of concerns

about these new forms of payment. Convenience is, of course, something we value, but it is not the only thing.

For example, how do you make the point that you didn't authorize something? There is no signature, it's a contactless use of your credit card, there is no pin if you are using a debit.

Now that they are making these cards that will be on your key fob, it is easy to misplace your keys, to set them down, have someone else pick them up, and anybody can walk through a contactless terminal and spend your money.

I know it is only up to $25 at a time, but you can still wipe out a lot of money in a hurry by misusing this.

I am be no means a technical wonk, but I understand that folks have been able to intercept the information from the RFID chip on the contactless card without being very close to it.

I was interested that Mark talked about the fact that they are going to ship the cards in a sleeve. I guess there will now be a big market in manufacturing billfolds and purses that have a shield so that it is safe to walk around with your cards that have a chip in it that broadcasts to any reader

at all times.

Other concern we have is about turning your telephone into a billing mechanism, either with the mobile phones or with your old fashioned telephone bill.

If you are going to use your phone bill as a credit card, then you need credit card protections. You need to be able to charge back any unsatisfactory transaction, and you need a dispute process.

We have gotten the use of phones and phone bills as payment mechanisms way ahead of the consumer protections.

MR. BURG: So we have two more presenters. I wanted to give James from Black Lab Mobile and Dave from Microsoft a moment if you want to provide a rejoinder.

MR. LINLOR: As far as with Bill My Cell and with different types of mobile payment systems like, there is a pin code involved.

Visa is part of one of the systems we use. They are very good at being able to use different types of velocity tracking and other methods for avoiding fraud. For one thing, if it is not an RFID system you can't spend a bunch of money.

As far as on the RFID side, I agree with what

Mark is saying, that there has to be a reasonable level of protections. I think that with the pin codes, with the type of location information that the risk can be limited. It will never be zero.

There will be a learning curve, an adoption curve, and it will be an ongoing process that has to be worked out. But there are reasonable protections right now.

The main question is what information is stored, how is it transmitted and, as you are inferring, I don't believe that anything is broadcast around.

The way the chips actually work is they are a query-challenge-response. So it is more secure than the impression might be given.

MR. BURG: 30 seconds.

MR. TURNER: It is a very short answer. The perception does not match reality to the extent that the press likes to play up the issue, not that we don't have some issues, but I think we are better off than it is often represented.

I will essentially assert the same position Mark did. If we do not provide systems that are fundamentally secure, we will not be in business either.

MR. BURG: We have a poll, I understand. This is going to be on the screen.

The question for all of you with your handheld devices is which of the following payment devices would you most like to use to make payments: Number 1 is contactless credit cards; number 2 is your mobile phone; number 3 is fingerprint; number 4 is traditional credit card; and number 5 is cash. Actually, A, B, C, D and E.

And the winner is traditional credit card, sponsored by Visa.

So the third part of our panel discussion is we will look at solutions to concerns about new payment mechanisms.

Our first speaker is Mark Kirshbaum, president of Experian Fraud Solutions.

MR. KIRSHBAUM: Thank you very much, Elliot, and thank you to the Federal Trade Commission for hosting this session, and thank you for those in the audience in Washington as well as those on the Web for your interest in this subject.

I would like to talk briefly about the trends we are seeing and then talk briefly about the tools that are being used to help protect consumers and to ensure that fraud and identity theft is kept to a

minimum.

First, what is the magnitude of the problem? I throw up a couple statistics for you to see.

More than 10 million Americans have their identities stolen each year. More than 80 million Americans have had their personal information compromised since February of '05.

And 13 percent of new U.S. accounts will be opened online by 2010, versus 3 percent in 2006.

You see the increased adoption of using online as a method for opening accounts.

And then lastly, that it's estimated in 2006 ID theft losses are $7.5 billion, and the vast majority of that is being absorbed by financial institutions, as you heard some of the other speakers mention.

When you look at these stats, you need to be very careful to understand what is the real meaning behind them. One indication is that 80 million persons who have had their personal information exposed, that actually is very inflated.

You need to realize that 26 million of that comes from a Veterans Affairs loss of data, which never led to any compromised data, and another 40 million came from card systems, which was later

revised downward to around 400,000.

Right there you could take approximately 66 million of the 80 million out, and you begin to understand what is the real magnitude of this problem, is the data really being used or is there just some lost data that is taking place.

What is being done today to protect and prevent fraud? First of all, recent statistics indicate the incidence of ID theft is actually leveling off, if not declining.

There was a 2006 Synovate survey, the FTC said ID theft and credit card complaints were each down 19 percent between 2003 and 2005, the message being there are tools being used out there in the marketplace that are actually working.

Javelin also says in their report that the number of ID theft victims did not actually increase between 2005 and 2006. I would tell you that the progress is due in large part to greater use by the commercial sector of third-party fraud scoring models and other technology solutions, including neural networks.

I would also say that consumer awareness and proactive monitoring is important. Those who take the opportunity to regularly monitor their credit as

well as review your bills and make sure the charges you see are actually made by you and also financial institutions utilizing data, analytics and software. Their motivation is to protect their customers.

As you heard before, if the customers are not willing to adopt the technology or do not feel safe, they will move to other methods.

Also, the institutions are interested in managing and reducing their losses and their risk and, of course, complying with laws because there are laws that must be complied with in this market space.

When you look at the tools that are used for the authentication space, it really boils down to one simple thing. You want to make sure that the person is who they say they are, period.

There are authentication factors and conditions, properties or parameters that can be independently tested to confirm that someone is who they say they are. It can be based on something you have, something you know or something you are.

You can see from the list up here that there are different methods of this. Something you have could be a card, a token, a phone number or an actual machine credential.

Something you know, think about the password

that's in your head, the answers you might have to specific questions that you are most likely to be the one to have the answers to, or it might be your Social Security number.

Or something you are. This is where you get into the space of biometrics, and I will talk about this in a second.

One of the ways to increase consumer protection through authentication is to actually leverage multiple factors of authentication through a combination of things that you have, things that you know or things that you are.

You can see a couple combinations here. As you will see, you could be using a combination of your card with a pin. Of course, you can use that online, over the telephone or other methods.

You could use a combination of your employee ID and a token. You could use an account number and a user password.

And you can see as you get into more stronger methods of authentication you can actually use what is called knowledge-based authentication or multiple choice questions and your fingerprint. Again, looking at a combination of these make up what is called multifactor authentication.

I will just mention briefly a couple last points. Quality data is key. It is incredibly important that the data come from reputable sources and that we have more information, not less information, that will actually tie an individual to their method of payment and to who they actually are.

We need to leverage-share data. That equals the best practices and provides the ability to view intra and intercompany data and to protect consumers.

The science of analytics and fraud scoring, fraud scoring models are used with data to determine the relative risk. These are not meant as a last point to make a decision as to whether you are going to get a card, whether a payment is actually going to go through, but it is a warning mechanism that can be used to perhaps do further authentication.

Thank you.

(Applause.)

MR. BURG: So in a way we are going to circle back now for a moment to the world of automated clearinghouse payments that Jeanne Hogarth talked about.

Elliott McEntee is the president and CEO of the National Automated Clearinghouse Association, NACHA, and he is going to talk about a program to

change the way these bank debits are authenticated.

MR. MCENTEE: Thank you, Elliot. The first thing I want to say is you have a wonderful first name.

Good morning, ladies and gentlemen.

I want to thank the Federal Trade Commission for, number one, putting on these important and, number two, for inviting me to participate.

My primary objective this morning is to share with you some exciting news. The banking industry is working on a new product that we think will help solve one of the products that we discussed here up to this point, and that is the possible inadvertent disclosure of account information.

We are working on a product that I will share with you some of the details in a couple minutes on how a consumer could make a transaction over the Internet, whether it is the purchase of goods and services, to pay your bill, to pay taxes, to pay a parking ticket to a government agency or transfer funds to another entity, make all those transactions without ever disclosing the account information to any party involved in that transaction.

Before I do that, let me briefly describe what my organization does, NACHA. You have heard of

Visa and MasterCard. We are the banking industry's equivalent to Vista and Mastercard for ACH transactions. The best known of these transactions is direct deposit.

I'm assuming that virtually everyone in the audience today gets paid by direct deposit. If you don't, please see me at the end of the session. I will try to sign you up.

What we do is we write the operating rules, much Visa does for their transactions for direct deposit. One of our rules, for example, requires the financial institution to make the funds available on payday at the opening of business, which is far more comprehensive than the protection you find in other federal consumer protection regulations.

We also work with banks to develop new products. I will be talking about one of those new products in a minute.

One of the real keys to acceptance of a new product -- and it was mentioned by several panelists before -- is consumer acceptance. And you don't get consumer acceptance unless you have consumer protection. The consumer has to feel comfortable in using that product or it is going to fail in the marketplace.

What's the problem today with Internet payments? There are hundreds of millions of payments made every year over the Internet.

The big problem as far as we are concerned is the consumer must disclose sensitive account information. That could be a credit card number. It could be a debit card number or could be their checking account number.

They may have to disclose that to a merchant if they are buying something, to a biller if they are paying a bill, to a government agency, like I paid a parking ticket in Washington, D.C. online with a debit to my checking account. I had to disclose to the District and the third party that processed the transactions my checking account number.

I must admit I was a little bit nervous doing that, even though there is lots of consumer protections if there is a problem. The concern is when a consumer discloses this information to parties they don't really have a lot of confidence in, they don't do a lot of business with, there is a possibility the account numbers could be compromised.

Everyone has read stories about millions of account numbers that have been compromised as hackers have gotten into computer systems operated by

merchants or, more commonly, into systems operated by third parties.

Visa, Mastercard, NACHA, we have stringent rules on how that data is supposed to be kept secure.

On occasions the merchants and third parties do not follow those rules. Hence, the numbers are compromised. It leads to a very negative consumer reaction. It may lead to terminate the fraud.

The banking industry will make the consumer whole, but the consumer feels very uncomfortable. They might feel violated that someone went into their account and used their account when they were not authorized to do that.

What's the solution to this problem? We think the solution is to develop new product, and we are working on developing such a product that would allow the consumer to make purchases, pay bills, transfer funds online without ever disclosing your account number information to the merchant, biller or any other party.

I will show a demonstration in one minute. Let me just tell you what you are going to see on that demonstration.

Now, I understand that people that are participating on the Web, they will not be able to

see this demonstration. But they can link on to this Web site and they will be able to follow the demonstration on the Web site.

A consumer is going to purchase some CDs at a Web site called Maestro Music. They will check out like they normally check out. Instead of selecting the normal payment instrument, they will select something called PIP, or payment in private.

The consumer will be redirected through a secure network to their bank. The consumer then will be logged in to the home banking system at their bank, and then the consumer will be authenticated by the bank, and the consumer then would authorize the transaction.

Now, while that is all taking place, the network that is moving the consumer back between the merchant and the bank has no information, does not see the transaction at all. That's the same thing with the merchant or the biller or any other third party.

That do I no see the exchange that's going on between the consumer and the consumer's bank.

If we can show the demonstration now. This will take about 25 seconds. But in reality, it only takes about 10 to 15 seconds depending on how fast a

consumer can click through this.

The consumer is now clicking out. You will see at the top of the screen it is PIP, this new payment instrument. They will select Gardiner Savings Bank which is a small bank in Maine. They will be directed to Gardiner. And that's the president of Gardiner Savings.

They are putting in their user ID, their password. All the banks are in the process of upgrading their authentication systems today. They will now submit the information.

The bank will authenticate the customer. The information is now moved from the Web site of the merchant to Gardiner Savings Bank telling about the purchase itself.

In this case, the consumer selected to pay out of the savings account. They will authorize the transaction, and now they will be redirected back to the merchant's Web site. It takes about 12 to 15 seconds.

Again, there is no information made available about the account number to the merchant, their network or any other third-party processors.

We have done a lot of consumer focus research on this, and there seems to be a high comfort level

with consumers, at least when we discuss this with them in focus group interviews.

A pilot test involving a couple dozen banks, a lot of merchants and billers will start in July of next year.

One of the keys is we will be evaluating consumer acceptance. Will consumers use this new technique, will merchants and banks feel comfortable with it. A decision will be made sometime in the end of 2008 probably whether we will go forward with this and launch this product nationwide.

Thank you.

(Applause.)

MR. BURG: We will turn briefly to the subject of biometric payment systems.

Marc Kirshbaum is going to show a slide on the screen and Elliott will discuss the application of some of those solutions.

MR. KIRSHBAUM: Just a brief overview for you of the different methods of biometrics, and they are categorized in three ways. There is genotypic, which is basically genetics.

These are ones you might think of naturally as your voice, fingers, hands and facial geometry. By the way, some of the stuff gets really fun because

odor is one of the methods of authentication. Believe it or not, we all have our distinct smell. Some will deny it.

Behavioral is the second method. These are things that are trained. They are things such as your signature, the keyboard strokes, the spaces in between your strokes on the keyboard. And one of my favorite ones is your gait. If anyone is a Monty Python fan, the Ministry of Silly Walks, everyone has their own gait, and believe it or not try to get into the checkout line at the supermarket and show them your gait.

The third is randotypic or phenotypic, which is random variations that are developed when you are a child. These include some of the more traditional ones, such as fingerprint, iris or retina scan or vein.

And still one of my favorite genotypic ones that I doubt will be adopted is actually DNA, where each time you go and buy that CD, just prick your finger, drop a little blood on the computer, and you will be authenticated.

So who is using biometrics today? Obviously the government is a large adopter of some of these methods that might not be scaleable down to the

consumer level. And also end consumers are using it through trusted organizations directly.

I want to mention lastly that the ability to use biometrics is completely contingent upon authenticating the individual at the enrollment point. If it is garbage in, it's garbage out. You have to make sure the person who is actually enrolling is who they say that are.

MR. MCENTEE: Thank you, Marc.

There is actually a real operating system today in several supermarkets around the country. You can go in and enroll in one of these systems.

Pay By Cuts is the name of the most popular one, where you leave a fingerprint scan when you sign up at the supermarket, and you give the supermarket your credit card number or credit card number, and then when you want to make a purchase, you just roll your index finger across a reader. It than scans the finger, and if it gets a match, it then authenticates the customer and allows the customer to go ahead and make the purchase.

It is not a real payment system in the true definition because the payment system behind that is really either Visa, Mastercard or the ACH network. It is a means of authentication.

I don't know exactly how well it is working in terms of consumer adoption. I know one of the concerns that have been expressed by some people is that all the credit card, debit card and checking information is maintained by this third party. There is some concern about that.

But that's basically the most popular way today of a biometric technique being used in the payment system.

MR. BURG: There was one other solutions area that we were going to cover. Tom Keithley from I4 Commerce isn't here to do that.

James Linlor and Elliott McEntee agreed to at least say a few words about third-party billing mechanisms.

MR. LINLOR: There is a system, for example, called Bill Me Later where you can sign up on the Web, and the whole idea is again to be able to hold the information, similar to what NACHA was describing, in another location, to be able to use the location, IP address or whatever else and some type of small goods delivery so that there isn't as much risk.

You are not delivering a credit card number or having someone type in a credit card number. You

are basically setting up a type of online referral billing account. That's what I understand Bill Me Later to be doing.

The one thing to mention with biometrics and I know pay by touch and other systems, they had a thing in the newspaper yesterday about having school kids out in California pay for their school lunches off their fingerprints which is fundamentally something that I like the idea.

But the problem with biometrics is the backend system and the honey pot. Once the information gets disclosed, I can get a new Social Security number, but I will not cut off my finger. That's the problem. Once it gets disclosed, once it is out there, now you have a real problem, and the backend systems are not clearly locked down.

MR. BURG: Elliott, did you have something?

MR. MCENTEE: I will repeat, well, you have 10 tries. I wouldn't advise that, though.

MR. LINLOR: You have 20 if you take off your shoes.

MR. MCENTEE: Most of the third-party bill systems work pretty much the same way.

They are in business to authenticate the consumer to the merchant or the biller, and then they

use the background, the Visa, Mastercard or ACH system for processing the payments.

I think the honey pot analogy you used is a great one. Instead of disclosing the information across perhaps hundreds of merchants and third parties, you are concentrating all in one place. We do know that makes some consumers uncomfortable to focus all their account information in one location.

MR. KIRSHBAUM: There are other methods of biometrics, including voice.

One of the intriguing aspects of voice is it is a little harder to steal and the technology is good in terms of authenticating. You give them a voice sample. You might say "1, 2, 3, 4," and each time you use your method of payment or want to authenticate using your voice, there is nothing to even remember because they change what is presented to you.

So the next time they might say "please repeat 7281." So it is hard to lose, it is hard to steal, and it is not something that can be lost. Some of these methods might be more effective than actually once your finger is compromised, it is compromised.

MR. BURG: We have about four minutes left.

I would like to make a couple very brief points and see if anybody has a closing remark.

From a consumer protection standpoint, because that's what I do for the State of Vermont and with other state offices of Attorney General, it seems to me that among all the things that have been spoken of here in addition to private sector initiatives behind these payment methods and systems, there are at least three things that we should be doing.

One is we should be taking a look pretty aggressively at what the experience, what the track record has been overseas.

In addition to Australia -- and, again, I don't know what exactly the story was there because I couldn't hear it -- but some of these payment methods are, if not mature, they are often used in countries like South Korea and Japan and the Philippines, and it would be worth taking a look at the track record on acceptance, breach of privacy.

The cultures are different. So there may be a higher level of acceptance on some criteria. But I think we have a track record that we can look at there.

Secondly, I think that government, both state

and federal, need to look at the harmonization issue that Jean Ann Fox mentioned.

I think right now, without adding any of these new systems, consumers, at least people who are not lawyers in this field, are completely confused by what their protections are, what happens if there is an unauthorized purchase, what happens if there is a theft, what happens if there is a claims and defense situation, where if you buy something and it doesn't get delivered, you are protected.

So I think we need a grand unified theory here of procedure and substantive rights. That would be something good for government at both levels to work on.

And then, finally, there are a lot of people out there, maybe more in Vermont, but there are a lot of people out there that in terms of financial literacy are not extraordinarily sophisticated. There are a lot of sophisticated people there. We have the unbanked. We have rural folks that don't have Internet access.

It would be great to see some kind of private-public partnership around the issue of consumer education.

Right now Western Union is funding a program

through the AARP Foundation which is educating consumers through a calling center approach on the dangers of wiring money to strangers, for example, in response to a counterfeit check scam or a telemarketing call.

It seems there is room for a lot of collaborations like that because the state of knowledge in this area is pretty low.

With those thoughts, any last remarks?

MR. MACCARTHY: On the data security stuff, we think we need to have a federal bill there to provide protections. Our biggest worry there is merchant and processor hacks.

Our biggest message to merchants and processors is don't save it if you don't need it. Don't save the security code. If you don't need it, don't save it.

On the grand unified theory, we think that's a great idea.

What was the last one?

MR. BURG: Consumer ed.

MR. MACCARTHY: We have something called practical money skills for life. If there is a way of working with you guys at the state or federal level, we will play.

MR. BURG: Jean Ann.

MS. FOX: We need to be clear about the point of who is doing the protecting.

We appreciate NACHA's rules are better than they are under the Electronic Funds Transfer Act and Visa, Mastercard may offer zero liability in some situations for transactions.

But for consumers to really have confidence in the payment mechanisms that they are using, we need law and we need private right of action and we need enforcement in order for this to go forward to everybody's benefit.

MR. BURG: Thank you.

MR. TOMASOFSKY: It would be interesting to come back in five and 10 years and sit down with the same panel and ask where their products are then.

Part of the comment I made earlier is the business model, the adoption curve, what is the compelling reason why consumers should use this product.

We talked about six or seven bases points of fraud built into the system, if you will. The system is happy, not happy but we should at least be able to support that from a business model standpoint. If that stays the same, why do we need all these things?

We saw 39 percent of the audience here would prefer to use their plain old credit card.

MR. LINLOR: Just on the adoption method and coming back in five years, that would be very interesting.

Adoption in Korea, for example, LG and other manufacturers are making a cell phone that has a fingerprint reader on it so you can use multifactor authentication. There is more adoption in Japan so you can pay for a Coke or Pepsi by swiping your phone near the machine.

In South Africa and other parts of Africa, you are use your cell phone for banking transactions because the local culture adopts that. In Sweden and other Nordic countries you can use it to pay for parking.

So the adoption around the world has been great. The U.S. is actually the lagging group in this whole picture, which is an interesting item.

MS. HOGARTH: From a federal perspective, I have to say while it is desirable to have consumer protections, I think Jean Ann is exactly right.

We have been in a reactive stage rather than a proactive stage because in part -- and this is a cop-out, but remember I'm not speaking for the Fed --

you don't want to stifle innovation and creativity.

So it is a real two-edged sword. How do you foster creativity and innovation and at the same time provide some degree of consumer protection?

MR. BURG: This was a wonderful panel. I really enjoyed this. Thank you all.

(Applause.)

(Break and Technology Pavilion.)

MS. MULLIGAN: Good morning. We are going to continue right now with our panel on new products and new challenges.

To lead off the session, we are going to start with Commissioner Kovacic.

COMMISSIONER KOVACIC: I want to extend my own welcome on behalf of the FTC to all of you here and to thank, again, George Washington University and its law school for its generosity in cooperating with the presentation of the program.

When we go back through the now nearly full century of Federal Trade Commission experience with consumer protection matters, a recurring theme that runs through many of the discussions of the Commission's work is a concern that the agency lacks the ability to stay abreast of the current developments in technology and commercial

relationships that affect its ability to carry out its work.

What's wonderful about the program that's taking place this week is this is a conscious policy response to stay in a position to make sensible judgments about the appropriate direction of future policy.

What I would like to speak about today are how new product development measures affect policy issues within the jurisdiction of the FTC and to talk about implications, not simply of developments in digital technology, but other rapid developments in technology that affect the way we do work and to talk about possible policy responses. And in doing this, I'm speaking on my own behalf and not necessarily on behalf of my colleagues. Like Francis Albert Sinatra, I will be doing it my way today.

First, to simply consider the general phenomena that the Commission faces and other policy institutions face in making decisions about how to design consumer protection policy, and what we have, at least keyed up in many discussions in policy making, is a basic mismatch between the rate of technological development on the one hand and the capacity of the institutions through which policy is

implemented to adapt in time.

And in many respects, I think one of the greatest challenges for our agency is to adapt institutional arrangements to put us in the position to respond to policy changes.

Our policy framework in the institutional arrangements tend to be somewhat sticky in the way in which they evolve. And by contrast, the technology developments tend to be comparatively more fluid.

A particular dilemma we face is that often the impetus to change the institutional framework tends to be crisis. A difficulty with crisis is somewhat like going to a casino. When the wheel of institutional change is spun, sometimes you win, but sometimes you lose grievously as well.

And in part, what these hearings are attempting to do is to put in place a base of knowledge that permits us in a far more deliberative and I think sensible way to make adjustments that are not simply triggered by the fact of crises alone.

Let me talk about several phenomena that result from the fact of technological change, some of them in many respects quite positive for consumers, some being far more threatening.

I want to start with the example of serious

fraud. One of the disadvantages of the fact of quick changes in technology and the nature of technology is that the possibility for serious fraud has been magnified.

For all of the wonderful things that new technology discussed in these sessions does, there are some adverse consequences, perhaps the most strikingly, as discussed by other panelists this week, is the cost of committing serious fraud has fallen dramatically.

In the old day, you had to use the flow technology to reach potential victims. Now it is far cheaper to do so. Many more messages can be sent in a much shorter period of time. The cost of entering the business of serious fraud has fallen dramatically.

Many of the participants in this process are in many senses quite attuned to the vulnerabilities of the enforcement process. They are highly proficient technologically.

A great challenge for us is to hire our own technologists to offset them. They are geographically adroit. They operate in a truly global environment. And we have discovered they are quite adroit at identifying the seams in the

enforcement process and putting great pressure on those.

Many of them have no concern for reputation at all. That is, in the firms we deal with, we really deal with two baskets of firms, one very legitimate firms, concerned with reputation. But the gravest threat to us in many respects are firms or individuals who have no concern for reputation at all. Again, what they try to do on a regular basis is to exploit vulnerabilities in the system of enforcement.

The effect on the obligation of legitimate firms changes with the changes in technology. And I will use the example of data security.

The great marvel of the modern system has been that the adjustments in question permit expanded and accelerated flows of data within and across individual firms and certainly within and across individual jurisdictions.

The fact of technological change I think poses a number of dilemmas for firms deciding what level of practice and precaution taking is acceptable.

To use the example of data security now is the fact that encryption in a variety of ways is now

more readily available imposes an obligation on firms to adopt encryption approaches as a way of forestalling those who would engage in serious fraud.

In thinking about the appropriate level of due diligence where firms carry out mergers and acquisitions, is there a much more elaborate duty on their part to engage in a careful examination of the security protocols and suitability of the acquired firm as a condition of going forward with an acquisition and assimilating the firm's operations into its own.

A second concern simply involves the consequences of product complexity. A recurring concern on our part is whether we have the capacity institutionally to understand some of the developments that are taking place.

That is precisely why, among other steps, we are holding these proceedings this week. One of the great innovations of Commission policy making in the 1990s was the deliberate decision under Bob Petofski's inspired leadership to devote substantial resources to the simple process of stepping back and learning and understanding what's taking place.

One of my academic colleagues, Peter Swire, offered the very wise advice to me over the past few

years in many conversations, that in policy making in this area, it is very possible to make serious errors by doing both too much or too little.

Peter's exhortation in many respects was to suggest what is indispensable to making good judgments is to take the care and use the time to make an accurate diagnosis of what's taking place.

From the consumer's point of view, the fact of ever more elaborate and complex technologies offers both the possibility of wonderful products and services, but it also places great demands on their capacity to understand precisely what the new technology does, both in understanding the representations made in marketing and advertising about specific products or services, and it magnifies in many ways the role of intermediaries, guides who can navigate consumers through the array of choices, the complex array of choices that they face.

Indeed, it points -- particularly for matters of quality control, product design, it places a premium on developing sensible policies that allow firms to exchange information across borders, across subsidiaries that identify possible flaws in product design, especially for product repair mechanisms to make judgments about how product design ought to be

adjusted.

A further institutional complication is what I call the policy archipelago. In the United States and many other jurisdictions, policy making decisions are fragmented across an array of institutions.

In the U.S., we not only have an array of institutions that deal with the civil side of policy making, but in the case of serious fraud, power is shared with those with the power to prosecute criminally.

It is a consequence of the archipelago, not simply at the federal and state level with attorneys general and consumer protection departments, where public institutions deal with each other, there are many occasions in which we have sent boats across the archipelago to land on other islands, only to be repulsed by the inhabitants of those islands, who fight back with the vigor that surpasses that which you would see with the private actors who we try to regulate from time to time.

Internationally one encounters perhaps the same phenomenon. If you go back to my earlier slide about the manner in which policy making takes place, certainly for serious fraud, if those cooperative relationships are failed and are not made stronger,

those committed on serious misconduct simply always stay several steps ahead.

The fact of policy making fragmentation has a number of consequences. Not only do we have broadly distributed authority but in many ways we are beset with regulatory anachronisms.

We still labor at the FTC under an exemption for common carriers that was set in place many decades ago when you had a single telephone company, and the thought was why not have a single regulator to take care of its needs from time to time.

Whether we are talking about communications, financial services or any number of areas, we still labor under regulatory structures that were established suitable to an industry configuration from sector to sector that may have been appropriate in the early or mid 20th centuries but are no longer appropriate. And the dilemma is that the institutional arrangements have not been upgraded as the technology in the industry has changed.

As a result, we have highly imperfect cross-agency cooperation among federal bodies, between federal and state bodies and across borders. An enormous challenge on our part is to provide the synapses and relationships which the legislative

arrangements themselves provide with no explicit coordination mechanism.

A last challenge I want to emphasize is the challenge to build knowledge within our agency, within other agencies with related responsibilities to build a better understanding of the technology in question, hence the proceedings that are taking place this week, to engage in a conscious process in what I would call policy research and development, studies of individual technological developments and commercial phenomena, ex-post assessments of the enforcement matters to be brought.

This involves taking some percentage of our resources every year as part of the feedback loop that informs operational decisions about enforcement to learn about the industries in question, to not measure our performance simply by the number of cases we bring, the number of rules we promulgate, but to take time consciously and assess the quality of what we are doing and to understand the industry.

We are precisely in the position of a business enterprise whose success depends critically upon doing research and development. You can't imagine a successful pharmaceutical company that has an R&D budget over time of precisely zero.

We have to have a continuing investment in building our knowledge and making adjustments in our own human capital, where we don't simply hire attorneys and economists, but we hire technologists whose specialization lies in exactly the technological fields that we are being asked to master.

There is a need to continually improve our own procedures and investigative processes, which the agency has done dramatically from the time I first set foot in the FTC in 1979 to the present date, using a knowledge base in place to respond quickly when crises come, to have done the research ahead of time so that we are not running behind the crises trying to figure out what took place.

Because we will be asked to make responses to legislators and other policy makers almost instantaneously. If we have done our homework beforehand, we are in a position to offer sensible answers the their concerns.

Some of the possible policy responses, more effort I think to punish serious fraud, which the FTC has engaged in, to avoid the dangers that the new technologically complex and progressive marketplace does not become a market for lemons, to engage in

expanded cooperation at home and abroad, as I said before, to invest more in building knowledge and critically to improve what I fear is the increasingly outdated legislative and statutory platform on which we operate.

This is why adoption of the U.S. Safe Web legislation is so critical in converting what is a fairly rutted two-lane highway into a fully divided four-lane expressway over which our programs can flow over time, to pursue changes and reassessments in the mix of skills with which we work, and to pursue greater integration between our competition and consumer protection, disciplines within the FTC.

My basic message about the entire path of policy development is to emphasize the close relationship between institutional design and substantive performance.

Simply put, the quality of the institutional arrangements through which we provide policy deeply affects the substantive quality of what we do. There is a great tendency when we talk about policy making to focus precisely on what I focused as an academic on in the classroom, the developments in doctrine, the substantive theories imparted to us by legislative commands, and too little effort devoted

to asking how's it going to be implemented.

Consider the following example. If I were to ask you would you like to go see Beethoven's Ninth Symphony tonight, you might ask who's playing.

If I told you it was a middle school ensemble that's long on enthusiasm, short on experience, you would find a way to decide to rearrange paperclips, pencils and other items in your desk drawer and possibly to read through old issues of the classified adds just to make sure you are on top of developments in the marketplace. But if I told you it was the Vienna Philharmonic, you would ask when and where.

In short, judgments about what agencies ought to do, should be doing can't possibly take place without a careful assessment of the capacity of the institutions to deliver the policy.

In this respect, I think it is a mistake to talk about best practices. To speak of best practices suggests a finite destination that once achieved needn't be reconsidered.

Given the fluidity of change in this instance, we are engaged in the continuing pursuit of better practices.

Indeed, for all of us, the best practice is the relentless chase for better practices. Thank

you.

(Applause.)

MS. MULLIGAN: I would like to thank Commissioner Kovacic for a wonderful setup for this panel, which was supposed to be opened, unfortunately, by Andy Moss from Microsoft Research. He is not here.

So Tom Jacobs from Sun Microsystems will step in to fill his place to give us a little bit of a technical background on what exactly DRM is.

MR. JACOBS: I think the best way to think about DRM is that it is intended as a technology for managing the rights for which people will want to use content.

There are many different ways in which DRM systems are being used. We are here obviously talking about consumer purposes.

That typically lends itself to talking about music or entertainment, about data types, but the same sort of technology is and will be used for the protection of your financial records, your health care information.

What DRM is intended to do is be a means by which either you or the providers and managers of your information will protect that data and either

provide access or deny access to that data. And they can do this by using cryptographic methods, as was described just a little bit earlier. It can be multi-key methods. It could be simply through watermarks.

Technology that we have learned about over the many years going back to protecting printed works is also being used. Rather than encrypting content with complex mathematical processes, you are simply overriding images that you can't actually see.

That's a way of making things easy to move around but you are not using that particular technology. There are also copy protection technologies where you put content out there and by definition you would be able to copy it once or copy it never. One example is the broadcast flags, a type of technology that made its way into legislation.

But there are many different means. The best way to think about this is when you turn on your cable television service, there is a rights management system associated with that. It is called the Conditional Access System. It is primarily designed for instantaneous use or denial of use of a service.

If you have an iPod or one of the consumer

electronic devices, those are using rights management systems which will allow you to use the content on a particular device for a certain period of time for a certain number of views or listens to a piece of content. These are all different methods by which DRM systems come about.

There are a number of standards that have come about in the past five to six years, some of them through the ISO community. There has been quite a number of troubles that have come about because of patents around this space. In fact, some industries, particularly the mobile industry, has chosen to not even deploy because of the costs associated with this technology.

So I hope that's a little bit of a brief overview.

MS. MULLIGAN: So we have been joined by Andy. I was going to suggest we give you a few minutes to elaborate on the technical aspects of DRM since that was supposed to be your slide. I had to take it all away from you since you are here.

MR. MOSS: Run in place, miss the opening and you are irrelevant.

One of the things to think about with DRM is to put it in context. Like many new innovations, new

technologies, often when it first hits the scene, it is misunderstood. It is either hailed as the silver bullet that will solve all problems or a scourge on humanity and is going to curse us to the dying day.

It is neither, obviously. What DRM really is, it is just a tool, like any other technology. Cars are tools for transportation that can be used to speed people away from accidents in emergencies or to help people get away from a crime scene.

It doesn't make the car bad. It just means the use of it is for good or for ill. DRM is very much the same way. What it does, what it is intended to do is give people choices.

I think when thinking about DRM -- I missed the opening. Perhaps you have gone through this already. There are a wide variety of things that go under the banner of digital rights management or copy prevention.

I think it is important to understand some of the distinctions as well.

When content protection technologies first started to hit the scene, they tended to focus on sort of prevention and limiting flow as a way to give copyright owners and content distributors a means to sort of control where they went a little bit more.

As we have gotten better at thinking about this digital world that we are all living in and trying to figure out how to make work for ourselves as consumers and technology providers, digital rights management has evolved to the place where it is less about inhibiting flow and more about enabling access.

The best way to think about this is not so much from big media protected but as you look forward, where are we going to be in five years and 10 years from now.

User-generated content is all the buzz today. What that really is all about is technology is driving down and declining the costs associated with creating and distributing content, which means more people are going to be in the position of wanting to make the choices about the content that they are now creating.

Digital rights management is the tool that they can choose to use or not to apply to a content they are creating so they can have a choice about where and how it gets distributed and under what terms and what conditions.

They have some sort of control over the content that they are investing in creating. So from a technology perspective, it is being used in a lot

of places today, everything from -- a variety of content protection technologies are used today, many of which you don't see. That's the best form of content protection.

A lot of people aren't aware they have been on DVDs for many years. There are a lot of examples where it has been used effectively. There have obviously been plenty places where it has been used less effectively.

I will leave it with the thought going forward that keep in mind when you are thinking about digital rights management -- I heard some of the examples around broadcast flag and some of the others -- we are early in the stages of this digital evolution.

This is very early on in our learning process as an industry, as consumers, at adapting to all the changes taking place around us. Digital rights management is a tool that allows us to take the world that's being digitized, all the bits that are being digitized, film, video, software, books, X-rays, CAT scans, MRIs, and being able to apply some control to that.

I think if you keep the context of it being a tool, maybe some of the hyperbole will recede.

MS. MULLIGAN: Okay. So our panel is going to work this morning, and I'm going to give a brief overview of both consumer expectations and some of the legal issues, primarily from a U.S. perspective.

Then we have a series of panelists on my right who will drill down a little bit more on particular issues around consumer protection, interoperability, security.

And then the second half of our panel is going to be about the obsolescence, the shift from analog to digital television.

Similar to the job you just had in trying to give a 3000 foot overview of technology of DRM, it is a little bit difficult to give a 300 foot overview of policy area of DRM, given that DRM is a technology that can be used in a variety of different spaces and, therefore, a variety of different policies and legal implications might flow from that.

The one that I would like to focus on today because I think it is probably most relevant to the FTC and most relevant to consumer experience, of course, today is around digital rights management technology in the realm of protecting copyrighted works, or we can think of them also as information bits. So music, video, whether it is consumer or

user produced or produced by commercial studios and increasingly other forms of information. So we can think about books moving into the digital environment more fully.

Copyright law, which has traditionally been the vehicle through which we protect the rights of copyright holders, provides a very limited set of what we call exclusive rights, the right to distribute, the right to publicly perform, the right to make derivative works, the right to make copies.

These rights are quite limited in scope. And within the realm of when a consumer walks home with a purchased piece of a copyrighted work, whether it is a book or a CD or a movie, they actually enjoy a whole lot of rights or they are allowed to make a whole lot of personal uses of that work that copyright says nothing about.

So when I get home with a book, I'm allowed to read it from the back to the front. I'm allowed to listen to the tracks on my CD. I'm allowed to listen to track 3 and then track 7. I'm allowed to read my book aloud to my child. I'm allowed to have five friends over to watch a movie in my living room.

There are a whole lot of things that -- copyright law simply says nothing about them. These

are the things, the personal uses, fair use, which is something that we have heard quite a bit about with respect to information, goods and DRM, is certainly a component of it.

So what can I do that might interfere with the exclusive rights of a copyright holder yet nonetheless be protected because we feel it has value, whether it is educational value or parity or criticism?

There is a lot of breathing space within copyright law. One of the effects of digital rights management technology is in many ways to invert this paradigm.

Instead of being a set of exclusive rights of the copyright holder, there is an extraordinary amount of flexibility around the personal uses that individuals actually experience in the home. DRM actually can turn this into what we would call a permissions culture.

So instead of having a work that I take home and can make lots of different uses of, the experience is that I might end up with a work that I can only play on one device. I might end up with a CD that when I put it into my computer, I actually can't listen to song 7 and song 10 or song 1, I can

listen from the beginning to the end or one track in the middle.

I might come home with a book that actually in digital format tells me I can't read it aloud. In many ways DRM is being used to give owners of copyrights increasing kinds of control over the way in which personal individuals use and experience copyrighted works within the confines of their homes.

Another big shift is the business models. Typically in the analog world, if we bought a book or CD or rented a movie, we weren't actually interacting with the owner of the copyright. There tended to be intermediaries.

Those intermediaries played a very important role. Booksellers, for example, have very strong allegiance to protecting privacy. If you all remember the Monica Lewinsky scandal and the fact that Kenneth Starr wanted access to the records of Monica's book purchases.

The producers of copyrighted works or the owners become the same people who are providing services, and we have actually seen an increasing use of digital rights management technology and other sorts of technical mechanisms to monitor how users are enjoying information goods in the privacy of

their own home.

Your computer could potentially be spying on which pages of the book you are reading or how quickly do you watch the move, whether you watch the whole movie or not.

Some of us might not be too concerned about this. But it is an important understanding that all of a sudden the removal of this intermediary provides new opportunities to monitor post-purchase consumption of goods.

So what's the role of law in the states and what do we know about consumer expectations? There is a wonderful survey I would encourage you to look at at an organization called Indicare that was formed by the European Commission but run out of the University of Amsterdam.

They did a survey of consumers in seven European countries. And some of the interesting findings were despite a limited understanding of copyright law, there were incredibly high clusterings around certain deeply held beliefs about the things they can do with copyrighted work, deep feeling that the ability to copy a work in order to move it to a different device was something that consumers should be able to do. Really deep interest in

interoperability, deep commitment to sharing. And sharing being very distinct from kind of the massive P to P proliferation that you might see, a distinction between what we might consider to be infringing and the typical experience of sharing a book with your best friend or sharing the music that you are listening to with your husband.

In the U.S., we have a host of different laws that are implicated in the use of digital rights management and the copyright space. One that has been of increasing importance is the Digital Millennium Copyright Act which basically makes it illegal for individuals to circumvent or to traffic in circumvention technologies that basically would crack the locks that have been put around digital content.

There is very little litigation at this point to tell us how the Digital Millennium Copyright Act interacts with consumer's desires to make personal uses or fair uses that might be prohibited or made technologically impossible by DRM technology.

We have seen some very aggressive efforts to use the DMCA to basically interfere with competition and particularly in ancillary markets. So with respect to garage door openers and toner cartridge

printers, not things Congress had in mind when it was passing this law.

But we have seen some very serious anticompetitive behaviors and patent misuse where people are trying to basically exercise control over ancillary markets.

Finally, consumers generally don't know what DRM is. That's certainly what we found in the European study. And right now when consumers purchase a work, there is little disclosure about the terms of that work that are being enforced, either technically or through a mixture of private contracts indicating how the consumer might use the technology, and it might interfere with the personal uses that they typically make.

So with that hopefully rather brief overview, I would like to turn it to James DeLong, who is the senior fellow at the Progress and Freedom Foundation, who will focus a little bit on interoperability.

MR. DELONG: Yes, thank you. I really see these things in a totally different framework in that copyright and its rules has been established largely in the context of technology and what technologies are possible.

For example, the first use doctrine which

says if you buy a book, that you can do what you want with it. Part of that is because you couldn't control the use anyway.

But think about it. Is that really a good doctrine for me as a consumer, in that I go into the bookstore, I see lots of books, 25, $30, and I sort of think maybe I would like to read that but I don't want to buy it for that price.

But suppose in fact the bookstore had a whole shelf of things that said you can buy this book and have it in your library for $30. You can buy it, buy the right to read it once for $3. I can choose.

I'm not really giving up any rights. I'm gaining some. This seems to me to be the basic story of DRM, and that is that simply by making more things possible, more price points possible, more different bundles of rights possible, you really unlocked a cornucopia of content.

The big problem now is creators are not paid enough. I'm not talking about the record industry, middlemen and all that. Creators aren't paid enough. Somebody makes a song, records a song, a cover, the songwriter gets 8 cents. I don't know what the musician gets. But every track you buy off iPod or on a CD, the songwriter, the creator gets only 8

cents.

You set up DRM, you get low transaction costs like the micropayments conference that will go on November 28th in New York. You get all sorts of different price points, different rights. And a lot more will go to the basic creator.

It seems to me that the crucial factor here is the transaction cost. A lot of people are working on that one, including the two gentlemen on each side of me now. Both Sun and Microsoft are companies that are totally dedicated to the proposition of interoperability in all its forms, and sometimes with each other, actually, yes.

The idea is that they need to draw on creators of software and programs, and in the words of Bill Joy, one of the founders, one of the truisms of the world is that wherever you are, most of the smart people are working somewhere else.

So you need to get them, no much how much you are willing to spend for talent. Microsoft, Sun and Google will spend prodigiously for talent, and they need to interoperate with those people.

They have to set it up so that you have some degree of control, so that you can have markets, so that you can have competition.

Now, I have one more analogy I would make, and that is to real estate. That is, the progress of civilization is intimately related to how much we have been able to slice and dice real estate rights.

You can lease things, you can buy things, you can buy them on time, you can have boxes in the air called condos. You can rent a restaurant seat for an hour. You can rent a beach property for a week. You can have time-sharing condos.

All these things make more consumer choice available. Think of the intellectual creations in that context.

The more different slices and dices you get, the more price points and the lower transaction costs, the more you can get. And of course these guys would like to charge you these monopoly prices but they can't do it.

They are working out through the market what consumers have to get as part of their bundle of rights. People do like to shift things from one computer to another. They are accommodating that. They are giving you the options.

If you let the market work, it will go.

One final comment, and that is there is another very practical element to all of this, and

that is I have one qualification for being on this panel and that is I was once a regulator in the Federal Trade Commission.

I used to help write trade regulation rules. I personally have been reversed by the D.C. Court of Appeals, also was once featured in a column the old Washington Star used to have called Gobbledygook.

I once rewrote a Commission rule in the form of a guidance document because it actually caused a few problems there which earned me a phone call from somebody at the Federal Reserve saying "you realize you just made every bank in America insolvent" and a trip to the chairman's office who looked at our guidance document and he said this is a very interesting way to do business.

The government, the FTC, no agency can possibly have the institutional capacity to keep up with this stuff. There is no rule you can write, no process you can follow.

As an example of this, Tom Hassa, a professor at George Mason has commented quite acidly on the Federal Communications Commission, that they suppressed cable television, they suppressed one thing after another, this is what will happen if you turn the government loose on these things, they will

suppress consumer choice, suppress this idea in the name of expectations and this cornucopia will be stopped up.

I will stop there.

MS. MULLIGAN: I will open it up for a question or two.

It sounds like we have perhaps a very positive view that the market is going to basically respond to consumer concerns.

What about something that copyright is quite protective of that perhaps the consumer marketplace might not respond to, things like the ability to reverse engineer? Do panelists have any ideas about what kinds of interventions are necessary or not necessary to make sure we have the leapfrog benefits to the consumer that flow from the ability of folks to reverse engineer each other's products and create things that are interoperable?

MS. MCSHERRY: I do. Corynne McSherry from the Electronic Frontier Foundation. When it is my turn, I will talk a little bit about some of the lessons that I think we can learn from DRM so far with respect to privacy and security.

And one of the key lessons I'm going to talk about and I think the key thing we can learn from the

Sony Root Kit fiasco of a year ago is it is extremely important that security researchers be able to have access to DRM and be able to freely reverse engineer so that they can essentially provide a check and protection for consumers, make sure there aren't security flaws in the multiple forms of DRM that are being promulgated.

Security flaws are being introduced into people's computers. One of the things that happened in the Root Kit situation is that independent researchers provided a key role.

They are the ones that discovered the problems. If they hadn't discovered the problems, with the help of a lot of folks gotten on Sony BMG's case about those problems, the problems never would have been fixed or possibly never would have been fixed. That I think is absolutely crucial.

MS. MULLIGAN: Please.

MR. MOSS: We are all standing on the shoulders of giants. We all work and learn based on everything that we have learned and experienced.

The focus on interoperability often gets confused thinking this thing has to talk to this thing.

From the consumer's perspective, what you

want is something to work. I pick up a device and whatever I have put on it should just play.

There are lots of ways to get there. One is to have my content protection talk to someone else's, and there are examples where that is already happening.

We work with cable technology and some of the DVD technology. There are examples where that is happening. Other ways are where the device has multiple forms of content protections.

That also works today, the key that you put into a machine sitting on top of your TV, it figures out whether it is playing audio or video and it is smart enough to know the difference. We will find that form of interoperability as well.

As we focus on the need for interoperability which is paramount, because from the perspective of someone who wants to distribute stuff, what you want is the biggest audience possible, you want to know that wherever you are distributing it, the machine that it ends up on is able to play it so you can get to the transaction you want.

So interoperability is critical. There are a lot of paths to get there. We need to maintain that focus.

The other point is in the world of digital rights management, trust is very important. You need to be able to trust from both ends of the transaction. If you are distributing something, you need to know that where it is going is a reliable trusted source and as the consumer, am I getting what I think I'm getting.

That brings up not only technical issues but labeling and issues around notification so that consumers know what the machine is that they are getting and the content that they are acquiring.

It is not a simple question.

MS. MULLIGAN: I will turn it over to Tom Jacobs, director of research at Sun.

MR. JACOBS: I agree very strongly about the need for interoperability, and I find myself in both camps of the discussion on it, because I believe that where we are today in this first generation of DRM systems that are out there is very much very closed, the architectures, the implementations, the security practices are not being reviewed in a broad and open way.

I think this "trust me" attitude of individual suppliers of technology puts at risk more Root Kit examples to come.

I think at the same time we can move towards more open, better reviewed, better analyzed approaches to doing security while at the same time maintaining trust systems.

You certainly want to make sure that you can't go and pick up an open source version of a DRM if you are a copyright manager. You want to make sure someone can't pick up the open source, rebuild it and hack all of your content.

There are trust systems and certifications and conformance prophecies above and beyond the source code implementations of things that would allow for trust, allow for these uncompromiseable systems without them being trusted to a single vendor.

There was a discussion earlier on about there has been a lot of troubles with Web browsers and the security that they provide. The ones that are more open are the more secure ones that are out there today.

So I think going in that direction with the next generation of rights management systems, where you get interoperability by design, as opposed to bailing wire and chewing gum of figuring out how you point devices at each other and get them to transfer

rights is what consumers will expect and demand.

MS. MULLIGAN: I will let you continue right on into your remarks.

MR. JACOBS: Just to continue on, where we are today with the iPods and DVD players that are out there today, this is really the first generation of true DRM systems. We have had copy protection and such systems before.

But if you think about where we are, we are much like where we were with the Internet about 10 years ago. If you stopped in 1996 and looked at where the Internet development was, it was primarily walled garden Internet service providers, and there were just a couple of major suppliers, AOL and Compuserve, as an example, who represented the Internet to most people who accessed the Internet.

If you had stopped there and tried to optimize for that world and pass too many laws for that sort of a world, we would be nowhere close to where we are today.

What you really need to do now is think about where we are going to be 10 years hence and what sort of protections and expectations consumers are going to have and where we want to go.

One of the comments that was made by Andy was

about the best DRM is the DRM that you can't see. This goes to the issue of if you look at this from copyright holders who are trying to optimize their financial opportunities or their use of their content in an exclusive way, the relationship they want to build with consumers for that content is one that's very cautious.

They need to be able to provide them with rights that they want to use on the devices they want to use when they want to use them. If they aren't using those rights, if they are not going to agree to those sorts of rights, they are not going to use the technology.

I go back to the discussion on security and financial instruments in the session before. People will vote with their pocketbook about the technologies they will choose. It is very interesting to look at the various studies that are going on about people who are using various DRM devices and then running into the problem that if I bought an iPod but now I love the new Zoom device coming, if I bought online for my tunes, I can't transfer and vice versa; I can't go between different devices.

As consumers get these problems slapped in

their face, they are going to want to have their rights become more portable or they will choose not to purchase from certain ecosystems of DRMs.

They might choose to totally abstain and continue to buy compact disks and figure out how to load them into their devices, which is what the majority of people do today because of the immense flexibility, it goes in my car, my computer, everywhere with me.

This goes to an effort we launched about a year ago called the Open Media Commons Effort which is intended to drive through open communities the definitions of interoperability by design and a big focus on accessibility and the royalty-free nature of source code implementations of DRM systems.

We have been working with the Creative Commons organization which has a different perspective on how you manage rights from an educational perspective and incorporating those models in.

The big philosophy thing we have behind this effort is rather than worrying so much about the device what we should worry about is our identity and various ways we can authenticate ourselves. But when I start acquiring rights, whether it is music or

video or my personal pictures that I have shot on my camera or camcorder, I want to be able to have those rights and manage them in the network in the same way I might use a Yahoo presence for my personal e-mail.

I can manage all of my e-mail and send things around by virtue of my network identity in that particular portal. We think when we move on to this next generation, it will be intraoperability by design as opposed to legal contract and perhaps market-limiting opportunities.

MS. MULLIGAN: I want to ask another question.

The notion of kind of seamless invisible DRMs sounds somewhat appealing. I want to take something home, and I just want it to work. I don't want to have to figure it out.

On the other hand, the invisibility of the Sony DRM that loaded a Rootkit on to my computer may be vulnerable, phoned home, the invisibility just didn't feel so good. It felt a little bit more like the design from Penopticon, where they are looking at me and I didn't know they were there.

I'm wondering -- certainly one thing the FTC has focused on in the area of privacy is notice, and particularly important I think where we have business

models that might be trying to radically restructure expectations.

Mr. DeLong set up the, well, you can buy one listen to the track, you can buy three listens to the track, the track can explode when you listen to it four times, share it with three people.

There was some interesting work, and I would point you to this Indicare survey, which showed that people are willing to pay twice as much for music that was portable, music you could listen to on multiple devices, music they could do lots of different kinds of sharing with than they were for very restricted, limited DRM-enforced rules, which is interesting but completely consistent with the theories of economists that talk about information flexibility being very aligned with information value.

I'm wondering what role might the FTC play with respect to making sure consumers know what they bought.

MR. JACOBS: The critical role for the FTC would be about consumer education in understand what technologies and commercial options that are out there.

One of the troubles with that is the end user

licensing agreements. The click-throughs seem to change with each new software revision. So if I knew what it was and read it once, I will probably ignore it the next time. So there's a problem.

Having the Trade Commission be able to stand up on the bully pulpit and educate consumers about what they should be expecting or knowing what they are not going to get by going certain directions will help to challenge the industry to meet those expectations and doing so from an educational perspective than from a legislative perspective.

MS. MULLIGAN: Can I push on that a little bit and get other people's thoughts? One is the rights expression language. We have to come up with some standardized way to allow us to talk about the rights we are going to grant, and then we have some enforcement mechanisms.

We are talking about the kind of cumbersome nature of trying to figure out what your rights might be or how you might be limited in your use of a piece of media based on copyright law, and they tend to be very long, difficult to comprehend.

Do you think there is a role for the same kind of standardization that has been core with respect to EULA so consumers are better able to

figure out what they bought?

MR. DELONG: One of the things that is interesting about the creative process is it has produced standard licenses so people have a better shot of figuring out exactly what they have. That is a great contribution.

MS. MULLIGAN: Your market analogy was about what choices they have, and the more we can reduce the transaction costs in that area, it would seem that it might actually help lead to more of a market model.

MR. DELONG: One of the things we worried about a lot was people who deliberately inject noise into the system, who deliberately confuse things so that advertising that was truthful and advertising oriented never went through. We never saw that. We left it for you.

MR. MOSS: The Rootkit issue I don't use. It is a piece of software that shouldn't be confused with DRM. It was in the context of a copyright owner doing something. But it was not part of the DRM. That was for clarification.

Consumer awareness is clearly something I think the Commission can help with. Consumers struggle with when I buy this, what do I get for it.

But it is not just the EULA. Obviously that needs to be clear in the understanding. But once you have acquired iTunes or software that allows you access to content, because of the variety of access and business models that are going to be implemented over the next several years, once they have the content, there also needs to be awareness of what did I acquire.

We focused on the user experience, making sure consumers know and can distinguish in the user experience when they are looking and discovering their content, how do they know which content has which set of rights.

Educating consumers to be aware that there might be multiple business models is part of the process. That's part of the innovation to figure out what works, is ours better than theirs.

That gives us the advantage because consumers find ours more appealing. I'm not sure you want to standardize that.

But certainly educating consumers they should be looking for that is a role the Commission can help in.

MS. MULLIGAN: I was actually going to put you on the spot, Jeannine, since you are here from

Consumers union and wonder if you have ideas on this particular issue.

MS. KENNEY: Okay, catching me off guard. In terms of just DRM generally --

MS. MULLIGAN: And thinking about whether there is notice, what kinds of information consumers might need to make good choices.

MS. KENNEY: That is obviously one of the biggest challenges, fair use concerns notwithstanding, is do consumers understand what they are buying.

I think it is pretty clear that right now they don't. Basic frustration of consumers who want to take a CD and use it in their car and find they are unable to. Consumers are experiencing that frustration right now.

When it comes to the disclosure issue, it is very difficult to fully disclose all the implications perhaps in a manner that FTC would be comfortable with to really foster the understanding of what a consumer is and isn't getting.

MS. MULLIGAN: So we have --

MR. MIRABAL: I want to make a point. You touched on this but didn't put your finger on it, privacy. A consumer, when they are buying something,

they are buying a service. They are not selling away their privacy in the process.

I think that is a very appropriate role for the FTC to be looking at in terms of what the discussion is today, because it is one thing to manage rights. It is another thing to do that in a way that it ends up invading the privacy of the consumer which that is affecting.

I think it is two separate things. Disclosure is one thing. Protection of privacy is another.

MS. MULLIGAN: And clearly an area where the FTC has a track record of activities. I will turn it over to Dr. Urs Gasser, the director of the Research Center for Information Law in Switzerland.

DR. GASSER: Thank you very much to the conference organizers for inviting me.

I'm delighted to be the European voice on this panel. The downside, of course, is I have five minutes to cover 25 countries which is an impossible task, I'm afraid to say.

The following will be a very rough overview and a rather fast-paced overview of the public policy debate in Europe. Before I start with that, I can't resist to comment briefly on the previous issue.

I think the privacy example or case that you just mentioned is a very good one because it also illustrates the limitations of the transparency-based and information-based approach.

We had a lot of hopes, especially in Europe, that if we only disclose what's going to happen with your personal information, if you already know what is going to happen with that information, then everything will be fine and consumers will make good choices. Unfortunately, it turns out it is much more complicated.

This leads us ultimately back to a normative question, actually, do we really want a system in place, an environment where, for instance, price discrimination takes place to the extent that you mentioned? Do we want users who will be able to make a copy for private purpose willing to pay twice as much for the same song as another person would pay without this right, if the current copyright regime and past treated both equally.

So that's only a comment, that probably the normative they mentioned should be considered as well.

Now let me turn over to the DRM debate in Europe. Over the past few years, much of the legal

and regulatory debate in Europe about DRM focused on the legal protection of DRM and technological measures because the member states were required to transpose the European copyright directive UCD into their national laws.

Now, introducing legal protection of DRM and harmonizing so-called anticircumvention laws across Europe has been an enormously controversial process. Three topics in particular have caused heated controversies.

We have already heard about it. The first one is DRM and its legal protection vis-a-vis traditional limitations on copyright, such as the right to make private copies; second, DRM and fair compensation; and third, DRM and intraoperability.

Given our panel's topic, please let me focus on the intraoperability issue. This topic in particular has gained much attention in the context of iTunes penetration of the European market, especially in France but not only there.

At the European level, however, no coherent DRM interoperability framework exists, although DRM intraoperability has been identified as an emerging issue by the European Commission.

This lack of cross-sectional DRM

intraoperability provisions leaves us with three areas of law that address this issue more generally, copyright law, competition law and consumer protection law.

Let's turn to copyright first. As I mentioned, the European copyright directive, like the DMCA you have mentioned before, mandates the legal protection of DRM systems. However, it doesn't set forth any rules on DRM intraoperability.

There is one recital that mentions that DRM intraoperability is something member states may want to encourage or should encourage, but the directive doesn't provide further guidance and seems to trust in the market forces, like some of our panelists today.

At the member state level, however, France has taken a much more proactive approach to DRM intraoperability.

A draft of the recently resized copyright act introduced an obligation of DRM providers to disclose intraoperability information upon request without being compensated. This, like iTunes -- it is not a surprise -- has triggered strong reactions by the media industry.

Accordingly, the final version of the law

softened up the original proposed. Now current French law states that a regulatory authority media interoperability requests on a case-by-case basis.

Under this regime DRM providers can be forced to disclose interoperability information on nondiscriminatory terms, but they have now the right to reasonable compensation in return.

Let's turn over very quickly to competition law. The baseline is competition law in Europe may become relevant in cases where a company with a dominant market position refuses to license its DRM standard to its competitors.

However, to date there exists no case law at the U level where competition law has been applied to the DRM interoperability problem. In France, there is one case where Virgin Media has tried to use competition law to get access to iTunes' fair play system.

The French Commission has ruled in favor of favor of iTunes, arguing that the market for portable music players is sufficiently competitive.

Finally, a few remarks about consumer protection laws. Three issues seem particularly noteworthy. First, the Norwegian Consumer Ombudsman has been very critical about Apple ITMS

interoperability policy. Second, a French court fined EMI Music France for selling CDs with DRM protections that would not play on car radios and computers, and EMI was considered to violate consumer protection laws because it did not appropriately inform consumers about these restrictions.

Third and finally, a recent proposal by the European Consumers Organization proposes to include -- and I think that's an interesting approach -- DRM in the unfair contract directive.

The idea behind it is that consumer protection authorities should also be able to intervene against unfair consumer contract terms if the terms are code based rather than law based.

So far, the brief overview.

MS. MULLIGAN: That was really wonderful. We will segue right into Corynne McSherry.

MS. MCSHERRY: Thanks for having me here.

What I would like to do is sort of fill in a little bit. We have been talking about privacy and security issues with respect to DRM.

I would like to fill in a little more background on a recent case that you are probably generally familiar with that I think can give us some lessons in terms of how to go forward, and that was

the Sony Rootkit fiasco is what we call it at EFF.

We were involved in some of the litigation against Sony BMG. So full disclosure.

In a nutshell, what many people don't realize is Sony shipped copy-protection software on 25 million CDs, two kinds of copy-protection software.

One of the things people forget is it is not just a Rootkit problem but there was another kind of software called Media Max that also had security problems. These were developed by two separate vendors.

The first sort of most famous problem, the Rootkit problem was that Sony was shipping CDs that installed hidden files on the users' systems. The second problem -- I'm sorry.

Before I close with the problems with that software which was developed by XCP, it also phoned home to the mother ship. It sent information about users' listening habits back to Sony.

There were some disputes about how personally identifiable that information was. There was no question that what was happening is it was establishing a connection between users' computers and Sony BMG and providing information about what users were listening to.

That was very disturbing for a lot of users who had no idea their privacy was being compromised in this way and maybe didn't want to be communicating to the mother ship just because they were playing a CD.

The lesser known problem is the Media Max problem. That was shipped on many more CDs. It installed software on folks' computers as soon as they inserted their brand-new CD without them knowing it, and then a licensing agreement came up, and even if you clicked "I disagree" on the EULA, the software nevertheless stayed on your computer and could even be inadvertently activated.

So that was a problem. In addition, there was a security problem with this software. The security problem with the Rootkit was it established hidden files on a system that a malicious hacker could then use. Basically they could fill in their own hidden files and mess with your computer.

What the Media Max software did is many of you in your workplaces will have standard security mechanisms where only some folks' administrators can make certain changes to the computer. This is really standard practice for administrators and low rights users, which are sort of the average person.

It is put in place to make sure that if any sort of drastic changes take place, an administrator knows about it and it helps fight off malicious attacks.

What Media Max, one form of the Media Max software did is it basically created a file that again a malicious hacker could come in and masquerade as an administrator and make changes to a computer that normally a regular user wouldn't be allowed to do. This was a concern as well.

Also, the Media Max software, like the XCP software, phoned home. It sent information back to Sony via an indirect vendor about user's listening habits, again, without their knowledge.

Those were some concerns.

Additional concerns were this, and I think this is something we haven't quite gotten to as much so far. Sony BMG was not very proactive in responding.

When the Rootkit issue first came to public attention, Sony initially responded by denying that it was a problem. We have had reports that Sony knew about it before it came to public attention and didn't do anything about it.

It was only when there was enormous public

pressure and lawsuits started being filed that Sony started providing updates and uninstallers for the software. They didn't investigate their other software, Media Max. It didn't go and look at its other DRM software and see if there was a problem.

Again, independent security researchers had to go and find out there was a problem, inform Sony of it, and then Sony did something about it.

This was a concern. You would think at that point Sony would have the incentive to be a little more proactive.

Let's face it. Content owners aren't necessarily the ones who will have the most motivation to do the security research in advance that they should do.

That's too bad, because when consumers buy things like CDs, they don't realize they may be potentially installing a security risk on their computer in the way they might when they install software that they get from Microsoft, where they expect updates and uninstallers and that kind of thing.

Content owners don't have the incentive to do it. Who does? Virus-protection companies and independent security researchers. So that's why, as

I was saying earlier, we think it is extremely important that there be licenses automatically for folks to do the reverse engineering that they need to do, to do the security research and provide patches and so on.

Finally, I believe we have been talking about disclosure. That is great. We think there should be disclosure before you buy. You need to know before you buy, not just information buried in an end user license agreement that pops up after you already have the CD at home.

MS. MULLIGAN: I want to ask one question to my fellow panelists, and then we will shift over to the second part of the discussion.

Sony was accused in many instances of basically operating as though they were spyware. They were downloading information software onto users' computers, not disclosing it, sometimes the software is being downloaded before the license agreement has been represented and, more fundamentally, the changes being made to the desktop experience, the security settings looked like the kinds of things like the Antispyware Coalition and Microsoft have participated in, the kinds of changes they say you shouldn't be making without an

extraordinarily high level of user involvement.

I'm wondering is there a bright line where we say you can't download certain kinds of software that are going to change users' experience, period, not because it is a threat to the consumer but the Rootkit, for example, created the opportunity for somebody to remotely turn my machine into a zombie and use it as part of a big botnet and engage in denial of service attacks.

I don't care if you want it on your machine; it is not good for the rest of us. Should there be any outer limit on what we can allow users to consent to when it comes to security settings?

MR. MOSS: I think it becomes a real challenge. We don't know today what we will be able to do tomorrow as technologists.

Any time you try looking for that bright line, the unintended consequence is preventing some future innovation that might be useful. I think that is a real hard thing to think about.

There are lots of ways that changing the user experience is a fine thing, where the user is aware, it is perfectly described to them, clear and it is consented, and then it is probably okay.

There are bad actors and people do bad

things. That's why as a systems manager, we constantly try to prevent bad actors from doing bad things. I'm not sure you can draw the bright line.

MS. MULLIGAN: As a former regulator, so the consumer basically just consented to the back door of their computer being permanently left open. Any role?

MR. DELONG: I'm not the FTC. Those come up in the P to P context, where the companies load you with all sorts of stuff and make you into a supernode, part of the system. In fact, if you are a researcher who knows what is going on and want to become a supernode, that is a good use of resources that would otherwise be wasted.

If you were helping to download all sorts of pirated material, the record industry will come at you because you have 10,000 songs on your computer and that's is not so good.

The problem of being a regulator so often would be it was this iterative process and you would pass a rule, and then all of a sudden more holes, so you pass more rules, and then you get the guidance.

You know what that's like. You can see the Federal Register. And I don't know how you regulate it.

One good thing about the Sony incident was the companies in the market did respond quite quickly. In fact, that problem was solved a lot quicker than it would have been by government regulation.

I really do have a lot of faith in exposure and a lot of faith in the ability of consumers when outraged to punish companies that they don't like.

MS. MULLIGAN: On the exposure issue, I actually represented one of the computer security researchers that uncovered a lot of this. The legal terrain we were operating in was actually quite complicated.

The ability to shine a light is actually quite complicated, given the state of federal law. I don't know if I will rely on the sanitizing effect of the bright glare of the spotlight in this area given the complexities of the research agenda.

Anybody have one last comment?

MS. MCSHERRY: It is not just federal law. It is also back to the end user license agreements.

The problem we see over and over, companies will shift their software where they need a license agreement that prohibit reverse engineering. That makes security researchers very nervous about how

much investigation they can and cannot do.

And that I think is in many ways a more significant problem than federal law as what is happening with contracts.

MS. MULLIGAN: We will shift from a conversation about a technology that most consumers don't know about to one all of us experience daily, I think.

Because I don't want to cut into your time, I won't say much other than a shift from analog to digital television is almost upon us, and there is a whole host of consumer protection and fairness issues, and I look forward to hearing your comments.

We will start with Manuel Mirabal, who is the chair of the Hispanic Technology and Telecommunications Fellowship, as well as the president and executive officer of the National Puerto Rican Coalition. And then we will turn it over to Jeannine Kenney, senior policy analyst, Consumers Union.

MR. MIRABAL: Thank you.

Most of the people in this particular room today are aware that there is going to be a transition in the way your televisions work from analog to digital, but that's not the case generally

in the public eye.

Most Americans today who for the most part own what is referred to as analog TVs and who are purchasing every year about 20 million analog TVs are simply unaware that sometime soon after Valentine's Day of 2009, if they don't have extra equipment or they are not subscribers to some cable system, they will have just snow on their television sets.

We have been working on this issue for a number of years. I know Consumers Union has. For us, representing a minority constituency, it is particularly important and alarming about what's going on.

In the minority community, all of the data we have indicates that minorities own more television sets and they watch more TV. They overindex in both owning and watching TV.

They also overindex in the amount of free over-the-air television that they use. In other words, they are not subscribers to some cable or satellite service. In the Latino community alone, 40 percent of the Hispanic community of Hispanic TV households use free over-the-air TV.

For the most part, two years ago when I was participating in the Nielsen minority viewer research

committee, when we did a study, a very small number of those Hispanic and African American households owned digital-ready televisions, meaning that for most of the minority community that our organization represents, it is going to cost them more to continue using their TV sets after the transition in 2009.

But more importantly, again, about disclosure, the issue which I think you were talking about is should the industry be allowed to self regulate? Should we rely on the industry to do the right thing for the public? Because if it doesn't, the public will respond and it will respond negatively to them.

In this situation, up until now we virtually have allowed the industry to self regulate itself in terms of how it is going to deal with the transition.

There is very little notice to a consumer today that when they buy an analog television set, which are still flying off the shelves to the tune of $20 million plus a year, that they are going to need additional equipment or some subscriber service to continue to have that work.

The bottom line is that television sets are not considered to be junk. They are not going to throw out three to four television sets. Most people

don't have the money to buy a new set, and many people don't have the funds to even buy the converter box that will allow their television sets to continue to work after the transition.

So the federal government has put into place a system where subsidies will be available through some system which has yet to be determined completely for individuals that have analog TVs and do not have another way of getting free over-the-air television to get a voucher to help them buy a converter box, which, by the way, doesn't today exist in any shape or form.

The industry, the electronics industry itself could probably if it wanted to today install digital conversion equipment in every TV they sold for maybe $15 to $20 extra, but they are not doing it because they are doing things the way they have always done it. When they can't sell those TVs here, they will continue to sell them in other countries that don't have this problem.

Our efforts in the last few years have been to bring to the attention of federal regulatory agencies like the FCC, like the FTC that there is a very important role they need to play on both sides of this, on the industry side and the consumer side,

and there has to be a mechanism established when all those phone calls start coming in to agencies about why their TVs aren't working.

We tried to convince Congress they are the ones that are going to get the brunt of these phone calls, because people are eventually going to find out Congress is the one that passed the law.

Let me close by saying we are not opposed to the digital transition because there are some important benefits that we will receive by using that analog spectrum for security purposes, to have first responders talk to each other in a more efficient and secure way by the sale of that spectrum which will produce some income which can be used for some other purposes, including subsidies.

What we are concerned about is the way this is going to happen, in particular, the way it will affect minority households who use their free over-the-air TV for local news and social purposes and other very important family kinds of uses.

So with that, I will turn it to my colleague here.

MS. KENNEY: Thank you. That's a really good setup for what I want to talk about.

I wanted to provide you with an overview of

the motivating factor behind the digital transition, how that affected the structure of the program that Congress created and what sorts of consumer issues that program structure implicates and then maybe close with a little bit of an outlook in terms of what the events of the last 24 hours may mean for addressing some of these issues.

Just a few starting observations. The title of this subpanel is obsolescence. It is important to recognize that the digital transition is government-mandated obsolescence.

It is pretty unusual for the government to basically render otherwise perfectly good electronic equipment useless for its primary purpose. So normally over time, technology transitions occur. As technology improves, the price goes down, quality is enhanced and adoption occurs.

Basically here a government is forcing consumers the adopt technology when they haven't yet seen the benefits.

What is interesting about this transition is because of the converter box issue that Manuel mentioned, those consumers who have least seen the benefits of the digital transition who are the ones who will most likely incur the cost because they

haven't adopted the technology.

It is important to understand the digital transition was budget driven in addition to being a government mandate. It was budget driven, although there were many members of Congress concerned about the availability of spectra for public safety.

What facilitated the transition was the need to grab the $10 billion-plus in spectrum auction revenues when the broadcasters had to return a portion of the spectrum. They are currently using simulcast.

The implication of that is Congress was looking to take that auction revenue and use it to offset tax cuts and program changes in other areas as part of the Budget Reconciliation Act.

This didn't occur through a telecommunications or spectrum policy act. It was part of a budget reconciliation process.

So that motivated Congress to try to minimize any cost associated with the digital transition program. But there was pretty serious recognition that you frustrated consumer expectations.

Consumers buy TVs expecting them to work. They understood there were political repercussions in how they did structure the transition. The first

question was how many sets out there are going to be affected. Sets unconnected to cable and satellite systems, but be careful, because we can't necessarily assume that yet.

There is nothing in the legislation that would allow cable systems to down-convert digital signals the analog. I am guessing Congress will address that or that will be resolved.

How many unconnected sets are there? Estimates have ranged from the low 20 million area to 80 million, which is what we found in the survey that we did. My guess is somewhere between 60 and 80 million unconnected sets. Regardless of what number you use, it is a lot of sets.

The other issue was how much compensation. We don't consider it a subsidy. You are basically compensating consumers for the cost of keeping their TV sets working.

How much compensation should be provided, partial or full and then to who? Everybody with unconnected sets, just low-income households, just those households that rely on over-the-air reception exclusively?

The way Congress resolved that is, as Manuel mentioned, they created a coupon program whereby

anyone with unconnected sets could get a $40 voucher to offset the cost of the box that would be required for their TV. They did not cap the retail price. We don't know how much that 40 bucks actually covers, which implicates some consumer concerns there.

Here's the problem. They basically made everybody with an unconnected set eligible but provided about a third of the amount of money required to meet the needs of all those eligible households.

They also structured the coupon program in a way that makes it pretty difficult for consumers to gets access to the coupons. It is a very short application window. The application window occurs about a year before the transition actually happens and the coupons expire in three months.

Basically NTIA has been charged with implementing an entitlement program with not enough money to serve those eligible. Congress provided $5 million for consumer education.

So let me see if I can summarize very briefly what the consumer issues are here. Obviously there is the fairness question, of being asked to bear cost for a transition you didn't ask for and may not want. There are a lot of risks here for consumers to be

misled and a lot of risks from misrepresentation.

HDTV is a very high-margin product. There will be incentive, we fear, for retailers to lead people to believe they can't buy an analog set, they need a digital set and you need an HDTV, when there are standard digital televisions or enhanced digital televisions that are perfectly good.

There will be an incentive to not let consumers know they can get a converter box. Obviously it is not an issue with consumers who are seeking to buy digital televisions.

There are some issues there with consumers not having enough information, not understanding the transition, there not being enough government money to really educate the public about what is happening and what their rights are for there to be some real serious issues at retail.

The other issue is price gouging. You have a combination of a final date after which your TV won't be useful, you have a captive audience and no cap on the retail price of the boxes. So we don't know what kind of games can be played at retail when there are no price controls on the technology.

The outlook, Congress was very concerned about inadequate compensation for consumers and how

that would implicate consumer acceptance of the transition.

I think given the flip in control of the House, we may see greater opportunities for Congress to come back and address that. And I say that because this was not a purely partisan issue. There was bipartisan support in the Senate for all eligible compensations, and they provided enough money to do that.

The House was a different story. There the Democratic members of the committee wanted full compensation. That was intentioned with the desire to maximize the revenues for offsetting deficit issues. So there was a split.

The result of the election may be that Congress will come back and deal with some of these issues in terms of inadequate funding for compensation, inadequate consumer education and some of the structural deficiencies of the program itself that may make the transition far more difficult.

At stake is the hard date. If consumer acceptance is low, there is the risk that Congress pushes that hard date back. That is something that certainly the electronics manufacturers don't want to see as well as those who are looking to use the

spectrum that's returned.

MS. MULLIGAN: I'm certain I don't want to be the representative whose district experiences white snow all across on the conversion date.

So I'm not always incredibly optimistic about the market to take care of certain things on their own. It seems there will be an enormous amount of push-back, the reality of all my televisions turning to snow.

What do you view as a potential role for the FTC here? I heard you talk about education and notice to consumers and fairness in marketing practices. I know there has been some experience internationally and a few other places that have converted. Are there things we can learn there?

MR. MIRABAL: There was the Berlin plan where they gave everyone assistance in getting converter boxes. I think Consumer Union tracks this one, what's happening on the Hill.

There was the sense I got that Congress was looking at industry, industry was saying to Congress we can't really get this done unless we have a hard date. Congress was saying we can't get a hard date together because we don't have the information.

I think they came up with a date that was a

little bit further in the future than the industry wanted it to be. It was a little too close for us because understanding -- let's take an example of the last few fiascos that government has managed to make for itself and just one that has nothing to do with the entire public but the enrollment in the Medicare program, which was very badly handled by a government agency which was underfunded, understaffed, ill prepared.

We are talking about --

MS. MULLIGAN: What specific impacts on minority populations?

MR. MIRABAL: Hundreds of thousands of people making phone calls. They will not call one or two offices. They will call as many offices as they can until they get an answer that says "we know how to make your television work."

There will be price gouging. There is going to be consumer rip-offs in small electronic stores. There will be misinformation.

For those individuals who are limited English proficient, whether it is Spanish or any other language, it will be even worse.

For the elderly, it will be something that will basically affect their lives because they are

even more home bound and connected to that television set than most other people. And many of them are on much more limited incomes with less flexibility to go out of the household, to file paperwork.

It is something that I agree maybe with this shift on the Hill that's coming that we need to go back and get the FTC and FCC to basically speak to Congress and let Congress know what kinds of experiences there are and what they need to address on this.

If that is not in place, we can't see going through with this because it is going to wreak havoc, not just on offices who will get these phone calls, but the quality of life of many, many hundreds of thousands of Americans are going to be affected.

In the end, it is just a pocketbook issue which can be resolved I think another way.

MS. KENNEY: I think as we move forward, assuming Congress comes back and addresses the deficiencies in the compensation program, deficiencies in education, I think there is going to be a need for vigilance in terms of retail practices, advertising, as well as representations at the point of sale, in terms of what consumers do or don't need.

There is all sorts of add-on equipment that

consumers can be marketed as well. You may be sold a new antenna when you don't need one. That is particularly important for vulnerable populations, the elderly, nonEnglish speakers who may not fully either have the ability themselves to adapt to the transition on their own or not have the information that they need.

So I think that's going to be an area that the FTC may need to focus on and I assume under existing authority.

I would note in the pending telecommunications bill in the Senate which may or may not be addressed -- I'm doubtful -- there were provisions that addressed concerns about false and misleading representations and practices associated with retailers and the transition.

I'm not saying all retailers are going to do this. I think there is a risk given the dynamics at play here.

MS. MULLIGAN: I want to thank all of our panelists. I think this was a really informative session.

(Applause.)

(Lunch and Technology Pavilion.)

MS. SHANOFF: All right, let's begin.

Hello, everyone. Welcome back from lunch to all of you. I'm Carolyn Shanoff from the FTC's Division of Consumer and Business Education.

We are the folks who try to give consumers of all ages and stages of life practical information they can use about recognizing and avoiding scams and ripoffs and understanding credit, being safe and secure online.

Since this panel deals broadly with communicating with consumers, we thought we would start by getting the consumer perspective. Let's go to the videotape and check it out.

(Whereupon, the video was played.)

MS. SHANOFF: Thanks to our consumers.

This panel is called the impact of demographics and shifting consumer attitudes.

During the last few days, you have heard many speakers refer to the increasing influences of the networking sites, word of mouth marketing, particularly among digital natives and millenials, and these are the people born between 1982 and around 2000.

We will hear from Bill Strauss, an expert on millenials, who will talk about who millenials will consider as far as communicating information, how

millenials will shape emerging technologies to suit their needs, what the implications are for the FTC and other consumer protection authorities and how millenials' concept of online privacy will evolve.

Then we will hear from Beau Brendler, Scott Shipman, Solveig Singleton. And after that my colleague, Eileen Harrington, will step up in about an hour and introduce part two of this panel.

Right now I would like to introduce Bill Strauss, a writer, historian, playwright, theater director, performer and authority on generational change.

With his partner Neil Howe, Bill has explored generational dynamics in several fascinating books I can recommend personally, "Generations," "13th Gen," "Millennials Rising" and "Millenials and Pop Culture."

MR. STRAUSS: Thank you. You forgot to mention two aspects of my background. One is that I co-founded the Capitol Steps, and the other is that I was a teenage capital page.

This is true. Really. This is Washington. Would I lie to you? And Mark Foley never hit on me once, and then I realized it must have been our vast age differential because at the time I was a tender

lad of 16 and Mark Foley was 9.

One thing about Mark Foley, as you look at what has happened in the government with the Democrats taking over, you can see with the tracking polls, the Mark Foley incident, the eruption of that scandal coincided with the time that the Democratic trend line started to head up.

There is an interesting millenial generational point to that, because as many of you will no doubt remember -- we certainly do in the Capitol Steps, recalling the jokes of 1983 and the page scandal then.

But those were Generation X pages, and even though that was on its face a much more severe kind of behavior that the Congressmen engaged in at that time, actually having affairs with pages of both genders, no one was forced to resign. There was no question about whether government should topple. Tip O'Neill was not hounded and his fitness questioned. Instead we went on.

When you get to millenials, you just don't mess with them. The fact that that was done in the context of IMing and text messages makes it all the more of an alarm.

We have something going on here with the

public aspect of this new generation that makes the subject today fitting. We also among today's teens have a rising sense of political participation and interest in the civic culture that surrounds it.

Some of the brightest young people I know who are brilliant at software design and Web community structures have pointed to the U.S. government's voting system as an example of older generations letting things get out of control, not having enough civic commitment to the task, not really being knowledgeable enough about the infrastructures and how that could lead to tremendous scandal and even a ruined election in the context of the depth of civic distrust that exists among today's older generations.

As we speak now, there probably are battalions of attorneys poised to invade both Montana and Virginia to make exactly that point.

I do often hear from younger people about how and why today's older generations have not used technologies to provide the kind of civic purpose that they see as their potential.

When you think about millenials, you have to realize that they have a unique position in history. That's how Neil Howe and I defined generations, in terms of that location.

Boomers were born just too late to have any personal recollection of World War II. That's why we actually define boomers, Neil and myself, as born between 1943 and 1960 because they don't remember World War II but they do remember Pleasantville while it was still black and white.

If you recall, the real commitment among Boomers about technology was to individualize it. The "do not fold, spindle or mutilate" slogan of the Berkeley free speech riot, which was actually the coming out party for the Boomers, then developed into an attack against the whole notion of the IBM mainframe computer, the idea there was some big brother, some massive thing out there that was going to control the lives of young people.

So they resisted that. Well, a lot of people think that the most famous ad of Superbowl history was the 1984 ad with the woman jogger smashing the telescreen. That was a boomer dream come to life.

The fact that Boomers were the architects in the era of the PC, the personal computer, shows that the penchant towards individualism that has defined Boomers has translated into the technological realm.

It wasn't something that you shared. It was something that you did to express your own inner

selves and your resistance to authority, your questioning mind, your creativity and the like.

Generation Xers came along, who were born in 1961 to 1981. They were the children of the consciousness evolution, the ones who were small at the time that we had so many changes in our culture and society.

When they collided with technology, it was back in the late '70s and early '80s, as computers were evolving and we didn't yet have an Internet, but we did have access to more digital tools.

What Gen X did with technology is to take the concept of the personal computer and the digital age and apply that to commercial life. They found ways of taking it beyond an idea, beyond a matter of personal expression and actually building businesses around it.

We have many, many entrepreneurs from that generation, from Jeff Bezos to Michael Dell to countless others who have built businesses around the notion of the successful commercialization of technology, entrepreneurial activities.

It is one of the things that has marked the generation that grew up at a time of rising divorce, latchkey children and declining trust in

institutions.

The number one institution in their life when they were young was the family, and that was struggling back in the 1970s as they passed through it.

By the time they were teenagers and young adults, they showed the greatest cynicism and the lowest level of trust of any generation alive at that time. That was the first time in the history of polling that we saw teenagers being more cynical than older people.

Then along come millenials, in 1982, the babies on board, the ones in the minivan. Those of you who have millenial children can recall the improvement in child safety devices. I have four children, two born in the '70s -- two Gen Xers, I should say -- and two millenials. And during the Gen X child era, the leading child safety device in a car was this. Or if you were a Gen Xer, it was this.

The whole notion was you have to protect yourself in this world, you have to handle things. That was the attitude toward school, the open classrooms, constant criticisms about how schools were failing and not turning out kids that were smart.

So guess who has been writing and reading the books for dummies because they figure they can learn what they need to do. By the time we got to the millenials, that was no longer acceptable.

There was a bright line that was drawn in the society for this new generation that was going to be very unX-like.

The whole goal of our society was to create young people who would reestablish civic life. In part, this reflects the desire of Boomers not to create themselves, but it also reflects a desire of the society to replace the generation that is dying, what Neil and I call the GI generation, the ones born in the first quarter of the 20th century.

They were the ones associated with very high levels of institutional trust. They also had been a generation that had been associated with using technology for civic purpose.

Recall the 1920s, probably the most rapid era of technological change in our country's entire history, when you have motion pictures, radio, public utilities, especially the car, the automobile, and how that transformed life in America.

These young people were the ones who grabbed hold of that technology. Remember all the Mickey

Rooney movies with jalopies and so on. That was something that they cared a lot about.

There was some concern among adults in the '20s and '30s about what all these technologies were going to mean for young people. If you look at the life story of that generation, another generation which had been born and grown up during the time after a period of rapid family cultural social unrest, 1890s and on, they turned those technologies toward powerful civic purpose.

We remember them as 50 and 60 somethings back in the years that we Boomers were growing up and going to college and the like. They actually were the ones that we were rebelling against.

They were the ones who were constructing those mainframes, those large organizations, the selective service systems using data as best they could to send us to Vietnam and whatever else was going on with technology. They were doing it for civic purpose and Boomers were saying no. Boomers were trying to disengage from the uses.

Well, as the millenials have come along, they have stepped into the same role that the dying GIs occupied, of taking a keen civic, rational approach to institutional life, toward political life, towards

the culture as well.

As they have grown up, we have seen a number of positive trends in youth indicators. Virtually every trend having to do with risk taking has declined.

Don't believe anybody who tells you that this isn't true. You can go to the core national data and over the last 15 years, whether you are talking about substance abuse or sexual behavior or crime or school violence, suicides, accidents, they are getting better year by year.

It is particularly so among nonCaucasians, but it is true for the generation as a whole. Meanwhile, most levels of achievement are rising as well, particularly math and science.

The verbal scores seem to be flat. Why are the verbal scores flat? It is because they are tested by the 20th century standards. You look at the SAT. It is a 20th century test. It is not a 21st century test.

They give young people a 25-minute written exam, a writing sample. 85 percent of them print it, 15 percent of them use cursive, and zero percent of them write the way people actually do these days, which is on a keyboard. Giving high school seniors

25 minutes of a writing exam is like giving them a driving exam on a horse.

But this is how we are measuring them. And we don't see these other things happening.

Clearly they have come along with the digital age. They have accepted that as their pad and paper.

To them, mobile technology and interactive technologies with user-generated content are what differentiates them from X. And there actually is a bright line. You can find with the 23, 24 year olds, "do you IM daily," "yes." But 25, 26 year olds, "oh, no."

Right now close to half of millenials who are online say that they use IMs over e-mail as a preferred form of communication.

There have actually been some surveys that show declining telephone use and a rising amount of IMing and text messaging. It is a little quicker.

Why wait for somebody to download an e-mail when you can text them or send them an IM and get it right away? So they have this different attitude about it.

When adults look at them and say you are disconnected from real life because you are always listening to an iPod or cell phone or laptop, young

people say exactly the opposite is the case.

They are more engaged and involved in social interaction than older people understand. They have these large sets of friends with whom they are sharing things.

The music industry has learned this, to its bitter discontent. These young people want to share music. They want to share it all the time. So they end up being sued for that.

I remember the U.S. Army tried to sue Boomers back in the '60s, and a lot of good that got them. Who are you going to bet on, 50 somethings in suits or teenagers with laptops?

But what you are seeing with them is a very powerful peer society that has a lot in common with what young people were doing with the technologies of the '20s and '30s. That was a very powerful team-oriented generation at that time as well.

You also are seeing a rise in a desire for institutional trust. It has been a very short time since we have been going from teenagers being the least trusting to being the most trusting.

Older people don't quite understand this. But teenagers and collegians have a higher level of trust in the government than older people right now.

And they are also the happiest age bracket. That drives 35-year-old script writers nuts, "how do I write programming for a generation of happy, trusting people?" Well, you have to write different kinds of stories.

I say as a comedian that one generation's punch line is the next generation's set-up line. Mark Russell actually once said to me something that I have found, and that is when you are telling a joke, if the joke has a cultural or social frame of reference, a person who is more than 20 years younger than you may have difficulty laughing at that.

I often hear 30-somethings say today's teenagers don't have a very good sense of humor. Well, hello, they have their sense of humor, they don't have yours. It is just how it goes in time.

You can actually look at the world as very ironic. Millenials think it's ironic that Gen Xers think everything is so ironic. It is not quite the same to spike your hair green and wear black. It is not quite the same as it used to be in the late '80s and early '90s.

What you see with these young people is they are sharing these technologies, they want to do that. Their strongest influencers are no longer ads or

celebrities but, rather, parents and their friends. That's really where the sweet spot of this generation is.

It wasn't that long ago we complained about young people watching too much television and being easily influenced by ads. Now we are complaining because they are watching too little network television and not being easily enough influenced by ads.

So you can see the whole point of this generation has shifted.

If you watch what the GI generation did is they passed through youth to middle age and their peak productive years and as they became family heads themselves, you can see that they really did make the generations that had been wild and raucous in their youth into something much more tame.

What Neil Howe and I are expecting to see from millenials -- and we see signs of this happening already -- is a renorming and a civilizing of the wild Web world that the older generations have created.

One of the major challenges for government is to include these young people in the official civic tasks of our society rather than battling against

them and to enlist the forces of history that are pushing in the direction of greater institutional trust in a way that will be useful to the young people and to history, actually, and not to get in the way.

We Boomers were very aware of when older generations were getting in the way of our agenda. The millenial agenda is not our agenda. In some ways it is a corrective against our agenda.

Now one thing that young people are focusing on in the realm of privacy, which is going to be discussed here today, is the problem of what some of them call oversharing. They can Google anything. They can Google you, but you can also Google them. And they are learning this.

And they are learning the dangers of the reputational downside of the Internet and of IMing and the like. The Foley page scandal was an example of that, something that came back to bite not just Foley but also the young people involved in that.

There are many cases that we hear of now where young people realize what I'm putting on the MySpace page can be downloaded by somebody with whom I am applying for a job.

What this suggests is that they themselves

are going to be looking for ways of taking our digital mobile, interactive, user-generated technologies and establishing new mores, new manners, new concepts for a modern civilization to take advantage of those.

I would like to close with a comment about technology that I got from a group in Berkeley, California. It they were organizing a conference. They were referring to young people. A lot of people talk about Generation Y. It is a very damaging term, because it keeps you from understanding what makes these new people new.

Think are not X plus Y equals Z. They are different. They were planning to do this conference on the declining manners and morals of today's young people and how they were wearing flip-flops and how they engaged in bad cell phone behavior and always doing IMing.

I was thinking how were young people behaving in Berkeley in the late '60s? IMing was "I am." And a flip-flop was probably the name of some little blue pill that you took. And a cell phone was something that you used to call home for bail money after you got busted. Figure that one out.

Anyway, what these young people are doing is

often misunderstood by older generations. You have to give them room, and you also have to give them room for what is going to happen out there in the larger world.

Realize we are not just educating them to be consumers, not just educating them to have a job or to be parents, but as I think we all sense, there is something brewing in history that will call on them to earn the subtitle that Neil and I gave them in our Millenials Rising book, that is, the next great generation, that there is some form of sacrifice, some use of technology, some reliance on institutional trust that is going to stand in their own life path when they get deeper into their 20s.

That's going to involve the global generation that they are part of. It is going to involve older generations as well. And whatever we do with them in technology we have to keep in mind there will be larger historical forces that will also intrude.

Thank you.

(Applause.)

MS. SHANOFF: Thank you for a great set-up to our panelists who will talk about changing trusted sources and what that means for consumer outreach and the focus on sharing among the people that you know.

Each of our panelists will speak for about five minutes, and then we will open the discussion up for questions, yours and ours.

We will start with Beau Brendler, the director of WebWatch, a program of Consumer Reports that focuses on trust and credibility.

MR. BRENDLER: Thank you for inviting me here.

I remember seeing a Richard Thompson concert here, and I think it was more than a Tech-ade ago. Although I am a Generation X, but I guess I can't be blamed for too much yet.

Judging by everybody's hand raising yesterday afternoon about recognizing Consumer Reports, I will assume that you all kind of know what that is.

WebWatch is part of Consumer Reports, and we do investigation and research on Web sites. We also do ratings of them and we also do some discussing of issues directly with consumers, which I will get to in a minute.

But to go back to this issue of trust or to focus in on this issue of trust, in 2002 we did a survey of Americans using social science methods to try to figure out what characteristics of Web sites generated trust among consumers.

In essence, what we came up with was identity, a phone number, an address, who owns the site, does the site actually say those things, advertising and sponsorships, whether it is easy to distinguish content from ads, customer service, currency and for.

Back in 2002 for Web sites and for consumers at the same time to say these are the principles that we have learned make for a relatively trustworthy Web site, the underlying principle being disclosure, don't hide anything.

Then a little later on in our history we worked with B.J. Fogg, who didn't get involved too much with stuffed monkeys at that time, but what we did do was we looked at a huge number of consumers. Everything I will refer to in terms of research you can find on our www.consumerreports.org, including this study.

We subjected a large number of sites to analysis by consumers to try to come to some determination as to which ones they thought were trustworthy, and then we did at the same time a study where we had experts look at the same sites. In essence, what we found out from the consumers was what B.J. hinted at kind of yesterday in his video,

consumers tend to be attracted by technology and layout and color, they think blue Web sites are believable.

To the experts, on the other hand, who are looking at health sites and financial sites, depth and expertise is important, sourcing is important and separates ads from editorial.

We did some follow-on studies after that and developed guidelines for travel sites and also for search engines and health sites. To touch on the research we have done over five years related to the trust issue, we just published a ratings of the 20 most trusted health information sites.

Of those 20, 12 of them rated either fair or poor. Six of them rated poor, and several of the ones that rated poor were ones that were directly sort of built by industry organizations. One was for Dannon yogurt. I have no objection to yogurt. And the other was for supplements.

The people who rated the sites was a panel of 19 people who were doctors, people who knew those types of Web sites.

The ways that people try to interpret on their own what makes a trustworthy Web site can be rather complicated. Over the course of our time, we

have had a lot of folks who call and ask us do you know this site is trustworthy, is it good or bad? And there are a few examples, in ascending order of complexity. It will make sense at the end.

We had someone call us up and ask if he could help us because he had gotten to a media site and bought a bunch of laptops and they hadn't arrived yet. Well, I'm afraid you are up the Danube without a paddle and we can't do much about that.

We had another caller who said I'm having trouble with this site, it is a prestige who's who guide and I'm a little worried about giving my money to them. We were able to go through the site with him and the site doesn't look too bad, but there was a phone number on there. We called it and the phone was disconnected. We also found out the directories, anybody can sort of nominate themselves and be in the directory.

Then we had some folks ask us about a site called www.courtrecords.org, which I will come back to later. I'm actually on the panel at 4:00. I will refer to that again. But we took a look at that site and had to pay money to join the site to figure out it was in fact a scam.

So we sort of took on the responsibility

there for actually investigating a site and helping a consumer figure out it was not in fact worth trusting.

The last example I want to give here is WebWatch Stopbadword.org, and this report actually came out today, I believe, from Stop Bad Word. This is an analysis they did. It was a site called Fake Mailer, installs a Trojan horse, claims to have no bundling but is bundled, redirects invalid Web addresses and is difficult or impossible to uninstall.

That's not nearly as bad as the site called FastMP3 SearchPlugin, which installs additional software without disclosure, installs Trojan horses, disabling Windows firewalls, redirects valid Web addresses, bundles applications, adds tool bars, changes users home page, displays pop-ups, compares computer performance and is impossible to uninstall.

That's bad. Those are out there. It is not all that easy to come up with a portable set of guidelines to give to consumers to say you can think about these things to determine whether or not this site is trustworthy.

Generationally, we do have some concern that younger consumers perhaps don't see as much value in

expert content, which is not necessarily a bad thing, but it can in certain circumstances lead to what one writer called the culture of an amateur.

McLeans Magazine -- it is sort of the Newsweek and Time magazine of Canada -- they just ran a very long article called "Pornography, gambling, Lies, Theft, and Terrorism, the Internet Sucks." It will raise emotions. In there they talk about something Wikipedia. It is funny. This is a Wikipedia entry that appeared and they observed it.

"On Wednesday, July 5th, Ken Lay" -- this is the writer of this piece -- "the former chairman and CEO of Enron Corporation, died in Colorado."

The news first hit the wires at 10:00 a.m., and at 10:06, Wikipedia proclaimed that Lay had died of an apparent suicide.

Two minutes later somebody changed the entry to say that Lay had died of an apparent heart attack and suicide.

Less than a minute later someone said the the cause of death was yet to be determined. At 10:11, the entry was changed again, this time asserting the guilty verdict had led him to suicide.

A minute after that, someone cited a news report that according to Lay's pastor, the cause of

death was a massive coronary heart attack.

At 10:39, one of the Internet's anonymous self-taught cardiologists wrote speculation as to the cause of the heart attack leads many people to believe it was due to the amount of stress put on him by the Enron trial.

Finally, a few hours later the entry was set straight. I was joking earlier with a colleague that we should go on there now and see if Wikipedia has named Bill Gates the new Secretary of Defense.

I don't want to be too hard on Wikipedia. But I do want to say that trying to develop a set of ideas or a map to help you determine whether a site is trustworthy or not can sometimes be difficult. I will stop there because I want to make sure my other colleagues get to speak.

MS. SHANOFF: Really a lot to think about and a lot to talk about.

Scott Shipman, senior counsel for global privacy practices at eBay.

MR. SHIPMAN: Thank you. It is a privilege to be here today with the FTC, the panelists and certainly the attendees.

My job is I'm essentially responsible for our global privacy practice for eBay, Inc., and that

entails PayPal, including Shopping.com and Rent.com and about 30 other brands.

I was asked to share my views today on trust, and I suspect it is because eBay is a brand that is well known and certainly to some level or another trusted by consumers.

I was glad to see, for those of you who were here on Tuesday, the video where the woman commented on eBay and she couldn't believe she was asked how people would buy in an anonymous, faceless transaction and yet look at the success that the Web site has today.

I won't mention that she was a plant, certainly glad to see that she said those comments.

From what I have heard over the last few days and even from what I have heard recently is with trust, trust is really formed and fostered by communication and choice. What I'm going to do in a minute is highlight some of the things that we do that I think help in that realm.

However, one of the things that I think is very important to keep in mind when you are talking about trust and communication and choice is that it doesn't mean perfect security. It doesn't mean perfect transactions. It doesn't mean perfect

reputations.

Software is hacked, mistakes in transactions happen, reputations evolve. I think the key to trust is communicating honestly and clearly and providing consumers with choices when those events happen.

I have heard a number of different things. So first and foremost, PayPal is blue. So PayPal is trusted. Another comment that I heard was that we are talking about the millenials and how they are sharing and they are sharing lots of information, and what I'm going to do here is step through PayPal, eBay shopping opinions and provide some examples as to how I think trust is really building and evolving, whether it is between millenials or Gen Xers or even my parents, the Boomers.

And I think that the notion, as you said earlier, with sharing varies as you go through those different generations. Sometimes it is providing that choice to those generations and other times it is not.

So to start with PayPal, in the prior conversation I was recalling the financial services panel that we had. There was a beta on paying without sharing your financial information. That beta has been in existence for about five years now.

That is called PayPal. You don't share your financial information with the person whom you are paying. That's the way it works.

The second part of that panel talked about mobile and other technologies. In fact, today if anybody on the panel wanted $5, I could text them with my cell phone right now and you would have $5 in your PayPal account.

Those technologies exist today. One of the key components is it is shopping, as we say, without sharing. You don't share your financial information with the seller. You don't have to worry about the waiter running behind the scenes and taking your secret code down on your credit card and coming out with a new computer the next day.

That's one of the enabling technologies that I think really helps foster trust.

Within PayPal, there are a host of other examples, such as buyer protection. Some people might say it is safer if I pay with a credit card. But buyer protection on PayPal, as long as you pay with PayPal, guarantees that purchase.

Cell phone payments, there was a concern that with cell phone payments that little code is not secure. In fact, when you make a payment through

your cell phone, you receive a text message back that confirms that you made that payment from your phone. You then have to provide an opinion to validate that payment.

We have an online safety center on PayPal that talks about how you can educate yourself. So in this case we are pushing a message to consumers. And as millenials really gather and soak up information, and certainly Gen Xers do the same, that's an area where they can self educate.

We also have two-factor authentication. To the extent people want that additional security token, they can do that.

Additionally, within the company globally we have around 2000 people working on antifraud techniques, not public facing but behind-the-scenes systems in place to protect customers' information. On top of that, as many of the industry leaders have come out, free credit report, free credit monitoring, so you have the opportunity to have free credit monitoring.

Again, it is about choices and it is about communication, providing the various customers with the opportunity to choose and select their level of comfort with a Web site. It is not just the fact

that PayPal is blue.

On the eBay side, I think there are some unique differences in addition to what PayPal is doing. That's been a challenge to the brand. When we look at our trust measurements, they are still very trusted brands. You say that must be a delicate balance and a tough brand reputational issue.

It is not about perfect security, not about perfect reputation. It is what are you doing, how are you communicating. When you look to eBay, it has a tool bar you can use if you are not on the site you believe you are on, and it will detect that, blink red and allow you to report that site to a network of companies that eBay has helped create that allows that site to be taken down by ISPs immediately.

When you enter in your password or eBay user ID on a site that might not be eBay, it allows you to say no, I approved this, this is a site that I do use the same password and user ID for, or "no, block this report and send that to ISPs."

We have fully deployed domain keys which is a way of authenticating our e-mail addresses. To the extent that you receive an e-mail and it has been authenticated, ISPs have the option to block that from ever even being delivered to you.

At this point ISPs aren't doing the blocking technology yet, but that essentially means every e-mail we send, to the extent it comes into your inbox, it is from us.

An additional choice is you can always go to eBay and review your message center to determine whether or not we sent the message. If it is not in there, we did not send it. You may have an e-mail that did not come from us.

Those are a few tools that eBay has within the eBay marketplaces. There is fishing tutorials and the feedback system within eBay, also within opinions and also within Shopping.com was at the time revolutionary and one of the critical places that allow consumers to buy in a faceless transaction.

It is not about having 100 percent feedback about each and every transaction you have had, but it is about what is the overall reputation, what are people saying about my transactions. When looking at sharing, that is open to the world. Anybody can view the feedback left by anybody else.

It allows the market and economy to dictate whether someone feels comfortable purchasing from one individual or another based on is it 99 percent, do they have a thousand feedback but are 999 negative

and therefore it's a net positive of one.

There are a lot of variables there that allow people to make an informed decision.

Lastly, jumping down to Skype, one of our newer companies and one we are still in the process of folding into the corporate development cycle, one of the things I also heard earlier -- I believe it was on Tuesday -- was the notion that people aren't really believing or contemplating the fact that if I have information at my house, naturally I know if the government is going to ask for it because it is at my house.

When I trust a service provider, when I trust a third party, they are storing that information, but I will not necessarily know if the government is asking for it. There is nothing that requires me to be notified that I'm using a third party and the government is now asking for my information.

One of the unique things with Skype is it allows people to communicate, allows people to communicate via phone, via video and chat, which is certainly one of the tools using to reach out to millenials because it is a way to push communication into a form that they are used to, whether it is a designated Web phone or whatever it might be.

The simple fact of the matter is those communications are encrypted and it is peer to peer which means your communication, your chat conversation is not stored in some central server that the government can access. It is a communication between you and whomever you are communicating with, whether it is 100 percent chat or a Skypecast, as we are saying. It is between you and those people, not between a central server, and, therefore, your information is really ultimately in your control.

So those are a variety of examples that I think all help show that it is about choices, it is about providing customers with lots of different ways to communicate, lots of different ways to trust, lots of different ways to pull information such that they can feel that a Web site is a trusted place or that a partner or that a buyer or seller is a good person to do business with.

MS. SHANOFF: Thank you very much.

Solveig Singleton, senior adjunct fellow and a visiting fellow at the Independent Women's Forum. She has written on how technology benefits women.

MS. SINGLETON: Thank you. I should also say I'm a rabid eBay purchaser, both a seller and buyer.

We are talking about trust and communications with consumers and demographics. I have three points I want to make.

The first is the demographics and the way it is changing is going to make traditional law enforcement very, very difficult. It is going to be spread really thin. But nevertheless, we are going to see really trusted and institutions of trust are not going to falter. The market will continue to support them, to expand them, as it always has, with all kinds of different feedback mechanisms.

First, as to the enforcement point. I'm a little skeptical of some of the generational observations about informal networks and peer to peer, because one of the phenomenon of all this mobile technology and so on and so forth in the hands of the new generation is as a general rule, they are not paying for it; their parents are.

So there are certainly avid users of all these devices, but what happens when they start having families and all of a sudden the iPod that they lose because they have left it on a bar for like the third time isn't being replaced out of their parents' budgets, it is coming out of theirs.

I think some of their behavior will change as

they get older. There will still be a lot of formal mechanisms of trust as well as the informal peer to peer ones.

Basically the demographic picture as a whole is really going to make traditional regulatory enforcement very difficult or almost impossible. There is not only the complexity of the technology, the mobility, the informality of it, there is the fact that the population of transactions and people online is going to be enormous, just the sheer number of small-value transactions.

A lot of these are going to be international, people buying very lightweight, easily shipped objects from other countries. Regulators will find themselves doing what they are already doing in the Spam context, which is they will bring some big cases.

This is important to set things right in those cases. But they will not be able to bring enough cases to have a substantial deterrent effect.

There has been a lot of research in deterrents in every context, from taxes to drugs to speeding to wife battering, and it also addresses the same thing, that what deters is getting above a certain threshold likelihood of getting caught. It

is not the severity of the penalty.

If you are below a threshold -- and we are certainly below that threshold, unfortunately, with Spam -- well, then, some other set of institutions is going to have to step in.

We have already seen the tremendous power of markets to respond to demand and shore up these trust institutions and create new ones. EBay is one set of example.

Generally this market responsiveness to demand is something that has been invisible. It is the invisible hand. It is invisible because we are almost always aware of it if something goes wrong, and the vast majority of transactions that are nothing out of the ordinary don't really get noticed.

But as this phenomena continues, there will be a lot more explicit trust institutions that are created by markets, insurance that is offered by PayPal, ratings, feedback. People will be able to see that part of it working.

There's another part of it that is going to stay invisible but I want to talk about in a little bit more detail. That's one of the strengths of how this market process works, is it assesses the need for trusted institutions by looking at what people do

much more than by what people say.

We have had a glimpse here up there of what it is people say when they are asked about trust, and some of their responses don't really seem to make all that much sense. But what you see in the market is what's the bottom line.

Are they clicking on the button, are they buying, are they not buying, are they hesitating over part of a Web site? What part of the Web site are they hesitating on?

The elections yesterday, there was a lot of polling beforehand, and as long as it is not push polling, it can be reasonably accurate. The bottom line is we pick elected officials by actually having the election, not based on the poll, because what people actually do when they go out to the polls is a much better way to learn about their true preferences.

E commerce sites have an opportunity to watch what people do all the time. They can't help but notice it. Someone is getting to a certain part of the Web site, and every single time they click off, or a lot of people hesitate before going through with the transaction. What's going on here? They have an opportunity there to respond.

One example, there was a national retailer who when people did a product search, they would always ask for a zip code, and the people noticed, "hey, when we asked for the zip code, they are not giving us it and they are going away. What are we doing wrong?"

People think that's weird. They haven't bought anything yet and you want to know my zip code, what's going on?

So we will tell them why we are using it. We would like your zip code so we can search warehouses in your area to see if the product is available. That was all they needed. No legalese, no boxes to check.

Just a little sentence and problem solved. People were like, oh, okay, now I see why you want my zip code.

So there's a tremendous amount that can be learned here from observing people's behavior. In this sense, often information is going to be more supportive of trust than privacy or anonymity in the sort of abstract sense, philosophical sense. People will make better decisions when they have more information, not less.

MS. SHANOFF: You have about two more

minutes.

MS. SINGLETON: That's fine. I'm almost done.

One of the perpetual things people bring up here is market failure. There's a growing economic literature where people are questioning a lot of the traditional theories of market failure and basically saying, wait a second, it is really not all that common, and if you think you have found one, you better check your assumptions, and chances are if you just wait, it will self correct.

Things that the market are not doing is an opportunity for someone to figure out how to do it and provide a service.

So by and large, the power of demand to get consumers what they want and what they need is really, really awesome. There are some weak points. One is, as you probably seem to have noticed in your own surveys, services and sites that are offering things for free, usually funded by selling advertising, the consumer isn't really the person they are selling to. The person they are selling to is the advertiser.

They are not as responsive to consumers in the same way. P to P downloading software is a good

example of that. It has led to a lot of people inadvertently sharing personal information to the extent people were mining peer-to-peer sites for Social Security numbers.

The Patent and Trademark Office is about to release a study on this. This has continued to be a problem, even though the P to P companies have denied it repeatedly.

The reason they are not responding to demand there is because the consumers aren't their demand. It is the advertising.

Just to close, market failure is the monster in the closet, but government failure is the abusive stepfather down the hall. It is much less a theoretical problem, it's coming but it is going to be okay.

MS. SHANOFF: Well, we actually don't have time for questions. We were going to have some questions. We were going to go out -- I have lots. But we don't have time.

We were going to go out with a song that Bill brought. Unfortunately we can't play it. There is a technical glitch.

Before we turn it over to Eileen, I would like you to say in a sentence or a word what advice

do you have for us at the FTC in terms of an institution like the FTC for reaching key audiences in the next 10 years.

I was going to say enough about you, let's talk about me, but we have no time for that. If you would give us your quick last best thought on how we can reach consumers with really key messages.

I think education is really important, sharing consistent messaging, really important. So for our organizations to work together, pretty key. I would like to hear what you have.

MR. STRAUSS: Number one, hire brilliant young people. When you hire them, listen to them, try to help them construct an infrastructure in which you can harness technologies for civic purpose and don't get in the way.

I think above all, I would respond to your point about millenials by suggesting that everybody think positively about young people. It really helps.

I don't try too much to speak for teenagers. I think what a teenager might say in response to your point of wasting money on the iPod, well, look at adults buying Hummers with all of the gas, realizing that they are globally depleting resources that they

will have to deal with over their lifetime, and wasting a little extra money on plastic and silicon chips is nothing compared to that.

MS. SHANOFF: I was young once. Thank you. A fine point.

MR. BRENDLER: Talk to as many real consumers as possible outside Washington and New York, and then I'd say enforce what things that you can and punish bad people and publicize it.

MR. SHIPMAN: I'd say partner with companies and communities with the people you are able to reach and embrace the technologies they are using rather than laughing at those technologies. So Skype-casts, those type, iPod, those types of things.

MS. SHANOFF: Thank you.

MS. SINGLETON: Design a game. There is a great one that's already out there where a child can play it, and their objective is to find a missing child, and they learn that way about dangers on the Internet and safety. So design consumer protection games.

MS. SHANOFF: Will do. Take a look at EnGuarde online.

Thank you very, very much.

(Applause.)

MS. HARRINGTON: Thank you very much. We are now moving into an area that is really all about trust, and that is privacy.

Before we go to the video, you all have your little polling devices. We will do a quick polling question here.

I understand that I can ask questions without any prior plan to do so. So here's the first question. Would you like to stand up for 10 seconds and stretch before we go forward? Number 1 is yes, number 2 is no, and number 3 is I prefer to keep that information to myself.

If we can get our polling up, get your polling device. Number 1 is yes, number 2 is no, and number 3 is I prefer to keep that information to myself.

Helen, you can make your way to the podium if you like. We are going to multitask here. Okay, 10 seconds. Don't leave your seat, stretch.

Now we have a little video and then we are going to hear from Helen Nissenbaum.

(Whereupon, the video was played.)

MS. HARRINGTON: We have a real polling question now.

What level of information are you comfortable

with sharing online? What kind of information of the following categories are you comfortable, most comfortable with sharing online?

Number 1, no personal information at all; number 2, name and address; number 3, name, address, phone number, e-mail address; number 4, Social Security number, date of birth, blood type.

Okay, there we have our results. Helen, that probably blew your whole theory. So you can come back and sit down.

MS. NISSENBAUM: I'm done. So I should start?

MS. HARRINGTON: Yes.

MS. NISSENBAUM: I should say from the outset that I'm a philosopher, just in case that makes a difference to what I say beyond this. But for the past few years, I have been working on a theory of privacy as contextual integrity.

I have published several articles, lately with some computer scientists, to formalize the idea rigorously and also working on a book. This theory says that preserving privacy is a matter of context, of respecting context-based norms governing the flow of personal information.

Now, I started paying attention to privacy in

relation to advances in information technologies around the time of Lotus marketplace households. That you may recall was a CD that Lotus and Equifax were going to collect of aggregated information about millions of U.S. households.

It was a philosophically interesting problem or event because, first of all, it rallied tremendous public protest by the Internet in particular. That was also quite new.

People resisted this technical advance and they thought it was wrong. They protested, and eventually the idea was dropped.

But the protest really didn't make sense in light of the prevailing theories and policies on privacy at the time, whose general defense was you protect privacy of private information. And the defense of this particular product was there was no private information, everything was already out there.

So either public reaction was misguided or the prevailing theories were missing something.

Over the next decade we didn't seem to be getting much better at resolving these controversial cases. You would see the same cycle go over and over again.

First there would be a new technology, something of great promise, new practices came forward, there was great enthusiasm. But at the same time, a lot of outrage from the general population, the privacy advocacy community. There was consternation and battle.

It didn't feel to me like a lot of progress was being made. I had a sense of being Bill Murray in the movie Groundhog Day.

So I decided that there was an important role here for the philosopher to play. We are not renowned for action. That was to try and develop a justificatory framework for answers to some of these puzzles that we were facing over and over again and that seemed to repeat in a particular cycle.

A justificatory framework would give structured reasons for resolving disputes, for guiding policy, for supporting some practices of others and for promoting certain elements in technology design. And in some of the other work I do, I'm very concerned about the values that are embedded in technical design.

I disagree with a speaker earlier today who talked about technology's neutrality. Let's call these outcomes. What sort of reasons could we give

for the outcomes that we wanted to support?

These reasons had to go beyond balancing interests, something that I call an economic approach. We didn't want to go in and only look at the stakeholder interests and decide how to balance these interests. And in fact, if you look at Lotus marketplace households, the legacy of that has been very disappointing.

If you look at Choice Point and Acxiom, we are so beyond the Lotus marketplace households that although there was a victory for the privacy advocates of that day, I would say that pales by comparison to what we are experiencing today.

What we want is research that all members of the political community can accept because they are grounded in social and political morality of our community.

Early on in my studies I came to believe three things. First, control over information by the data subject. We have heard it mentioned today that consumer choice is not the Holy Grail, though it is part of a large picture.

Number 2, the private-public dichotomy that so much of the work on privacy has adopted is leading us astray and it is holding us back in our efforts to

grapple with technology-induced puzzles.

Number 3, we were squandering a wealth of social information that plays hugely into people's assessments or judgments that a given activity or an application of a technology is a violation of privacy rights, but in my theory I call it contextual integrity.

These were the foundations of this theory called the theory of contextual integrity.

Now, this theory is not a discovery of something radically new. I believe that we all actually know about the ideas in this theory. It is an attempt to bring these ideas forward and also express them more systematically and make them a little bit more rigorous.

Indeed, what I want to do is draw your attention to a case in which the FTC was involved where the FTC had developed rules that were dealing with security and confidentiality and they were sued by Transunion and the Individual References Services Group. I won't discuss the details of the case.

The major point of disagreement was whether information and credit headers, including name, address, phone number and Social Security number, should be covered by the FTC's rules. The FTC said

yes and the plaintiffs said no.

The court decided in favor of the FTC. The move that was really interesting to me was that the court refused to draw a distinction between information that was somehow intrinsically financial and information that was not. Rather, it accepted the FTC's rationale that any information should be considered financial information if it is requested by financial institutions for the purpose of providing a financial service or product.

Now, there are four factors that are crucial to this theory of contextual integrity. My claim is that what matters to people when the flows of information and the changes in flows of information that are brought about by technology or particular technical systems or devices is and here are the four crucial factors.

One is what is the context of a particular action or practice in question? Is it financial? Is it health care, education, religious observance or social, family, dating, et cetera? Two, who are the parties involved and what are the capacities in which they act? And by the parties we have the data subject, we have the recipient of the information.

So is it a patient, is it a student, is it a

date, a customer. The recipient, a secretary, a professor, a parent, a friend, and the transmitter of the information who may in fact also be the data subject.

The third factor is the type of information in question, not just public or private but is it the physical condition, religious affiliation, how many spoons of sugar you take in your coffee, what side of the bed you sleep on and your sexual orientation and, of course, more and more and more.

And number 4 is something that I call transmission principle. That's the fourth factor that people are very attune to. And that is what are the conditions in which information flows from one party to another. Is it a condition of confidentiality? Is the information bought and sold? Is it given by the data subject under the data subject's control or volunteered by the data subject?

This is where control enters the picture. Is it given because it is demanded of the data subject and so on. All these transmission principles make a difference.

People are attuned to all four of these factors, and they are sensitive to them when they are making an evaluation that their privacy has or has

not been violated.

Apropos this little poll that we just took -- and, of course, there is a lot more to say here but I'm aware that my time is up. Eileen is nodding. I don't have another half hour to develop these ideas.

But I would recommend to those who are taking future polls, those who are designing technical systems, those who are making policy to ask questions about all four of those factors so that the next time someone asks you do you feel comfortable giving your name or your blood type, et cetera, online, I think it is quite appropriate to say, well, you need to specify that question more.

Of course, I would feel comfortable if it was my physician asking me to tell my blood type, knowing that my physician is bound by norms of confidentiality.

These kinds of questions that are being asked will not give us the kinds of information that we need if we want to know how consumers feel about their privacy. And I would love to see a lot of social scientists going into the variety of social contexts in which we share information to understand a lot better what these norms are and how we can move into the future with our new technical systems.

Thank you.

(Applause.)

MS. HARRINGTON: Thank you, Helen.

We have been having a very serious and public discussion about privacy at the FTC for over a decade, really, beginning with the hearings in 1995. Today we are unfortunately able to present only a few more facets.

We are trying to continue our discussion and exploration by looking at several different facets, some new to us, including Helen's discipline brought to the table. So thank you very much.

Now for a very different focus, Joe and Chris are going to present some research.

MR. HOOFNAGLE: Thank you and good afternoon, everyone. I'm Chris Hoofnagle from the University of California at Berkeley. I'm doing new work in preparing for FTC Tech-ade, and I was looking at the research that we were performing at UC Berkeley and I realized it was complemented greatly from Professor Turow of the University of Pennsylvania in Annenberg.

It also will be available online. It basically gives advice to the Federal Trade Commission about what challenges it must confront in the upcoming decade.

So we all know that over the past 10 years since the Federal Trade Commission's last forward-looking hearings on the global marketplace that the FTC has taken a market-based approach.

They have said we are going to let self regulation flourish. They have said we are going to have notice, choice and security, some access and accountability, and they made interventions for certain issues, such as children's privacy and telemarketing.

And the working assumption that the Federal Trade Commission has followed is if we have good information, if consumers have good information, they will be able to make good choices in the marketplace.

The slide show is working. Is self regulation working? I think that's a question that is worth a lot of critical inquiry.

We know that people care about privacy. If you can ask them about how they care about privacy, they will respond with very intense interest in protecting personal information.

But at the same time many economists will say people care about privacy but what really matters is what they do. They seem to care about privacy, but then they go online and they share their e-mail

address and blood type and Social Security number and do all these things that are not perhaps very smart and aren't very protective of privacy.

However, from experiments we have done at UC Berkeley, we do know that consumers take action to protect their privacy. But they are frustrated in effectuating their intent by a number of factors, their economic, their framing issues, their psychological issues.

And I think as we move forward into the next decade as information collection becomes less transparent, as people know less about how the business practices work and less about how the technology works, there are serious questions as to whether or not self regulation will protect people's privacy adequately.

MR. TUROW: We asked some questions at the Annenberg Public Policy Center. Each one had 1200 people in representative samples of the United States. The first one, they were people who had the Internet at home and the second one is people who had used the Internet in the last 30 days.

When we gave them the statement "I am nervous about Web sites having information about me," 70 percent in 2003 said they agreed or agreed strongly.

In 2005 it was 79 percent.

A number of questions were asked. There is a consistency that is fascinating. Consumers see both business and government as threats when we asked do you think these entities can help with your privacy.

92 percent worried about the commercial marketers and 83 percent worried about government. We asked the question in other ways too. There is a real concern about government protecting people just as there is private entities.

When we asked about the use of the term "privacy policy," we got a fascinating set of answers, again, in two separate years. We gave them the statement "when a Web site has a privacy policy, it means the site will not share my information with other Web sites or companies."

Now, we all know that's not true. In 2003, 57 percent agreed or agreed strongly with that statement. In 2005 we did it somewhat differently to see if maybe the phrasing had something to do with it. We asked if it was true or false. 59 percent said it was a true statement.

Beyond this basic misconception, which I think is really basic because people see the words "privacy policy," the label as having a particular

meaning, consumers hold many misunderstandings about marketplace practices online and off-line. As you know, the two are very much interpenetrating.

These are just some of the findings in our survey in 2005. These were true/false statements.

"Most online merchants give me the opportunity to see the information they gather about me." The answer is false. But 47 percent got that wrong. That is actually one of the lowest percentage of wrong.

"Most online merchants allow me the opportunity to erase information they have gathered about me." 50 percent got that wrong.

"A Web site is allowed to share information about me with affiliates without telling me the names of the affiliates." 49 percent got that wrong.

"When I give personal information to a bank, privacy laws say the bank has no right to share that information, even with the companies that the bank owns." 73 percent got of the people got that wrong.

Parenthetically, we asked a statement about fishing, which is not up there. The great percentage of Americans don't understand what fishing is.

"When I give money to charity, by law that charity cannot sell my name to another charity unless

I give it permission." 72 percent got that wrong.

"It is legal for an online store to charge different people different prices at the same time of day." 62 percent got that wrong.

"It is legal for an off-line store to charge different people different prices at the same time of day," and 71 percent got that wrong.

If you go to our study which is online at the Annenberg Public Policy Center, you can see the complex feelings and knowledge that Americans have about the notions of price discrimination when they don't know that it's going on.

Now, consumers also believe that many common practices shouldn't be acceptable. We gave them scenarios and one in particular where we said name us your favorite Web site, and we asked about the Web site and then we said what if the Web site took information, gathered information about you and mostly anonymously used it to serve you ads, a typical kind of information use policy on a Web site.

85 percent of the people when they heard that scenario rejected that common tracking information extraction and sharing model that we used on the Internet when it was explained to them.

And through a number of other types of

questions in that survey we basically came to the notion that Americans have very little clue about the data gathering and mining that goes on behind the screen.

They understand that data are being taken from them. They know they can be followed on the Web. But they really have no understanding of how individual bits of data can be used in technical ways.

MR. HOOFNAGLE: So the traditional retort to Professor Turow's findings is that people say they care about privacy, but they do, that's what matters.

This is how our research at UC Berkeley complements yours quite well. When we did a study of Internet users and we actually have a lab at Berkeley where we hire research subjects to do tests, 75 percent adopted at least one privacy protection strategy. That includes doing things like lying, putting down false information to hide their true identity when interacting on a Web site or withholding payment, not going through the transaction because they are concerned about privacy.

These results are supported in other aspects as well. We all know Professor Allen Weston, he put out a survey two years ago that said that even people

who say they don't care about privacy, the so-called privacy unconcerned, the people who say privacy is already gone, it doesn't matter, a very large percent of them took at least four of seven privacy-protecting tactics that Professor Weston presented to them.

Of course, as you get to the pragmatists, that number increases greatly. So people care about privacy. They are trying to protect it.

What we have done in the United States, hoping my slide goes, is we have relied on the idea that privacy notices will help educate individuals and help them make good choices about privacy.

However, when we studied a form of privacy notice, known as the end user license agreement -- this is essentially a contract which comes with the software -- people generally do not read them, and when they do read them and later install the program, they still don't understand key terms of the bargain and they still regret their decisions.

So at UC Berkeley one of the ways we have determined whether or not a privacy choice is good is we ask users after they have taken some action whether or not their choice was regretted. And huge percentages of individuals say they have regretted

the decision they have taken.

When you change the condition a little bit, when you give them a short notice instead of this big long EULA, it helps, but it is still not perfect. Huge numbers of people still say they regret the decision they came to relying upon notice.

Other research we have done and colleagues have done across the nation concerns psychological and economic factors that help explain why consumers do what they do.

One problem, one basic problem we all know is that notices are written for attorneys. They are too long. Even when people try to read them, they are impenetrable. There are information asymmetry issues. Individuals don't understand the terms of the bargain, especially when saying their product or service is free.

That leads them to think there are literally no costs, when in fact the cost of privacy can be quite severe.

What we concluded in the paper is these barriers taken together and the public polling research that Joe has done and the user interaction research we have done at Berkeley shows individuals need a helping hand, they want privacy, they say they

want it, they try to get it, indicating a need for a helping hand.

All these different factors frustrate their ability. We can only pay attention to so many things a day. We have kids, jobs, other responsibilities. We are too busy to pay attention to all these issues.

I'm going to move very quickly at this point. If we don't take care of this problem, what's going to happen is people are going to get notices and they are going to consent to spyware and put the entire network at risk.

We are beginning to see that with the Sony Rootkit and with other issues.

MR. TUROW: Things can get worse also if you look at some of these issues and bring them into the mobile world, the off-line world.

We make the mistake of thinking that the online world and the off-line world are separate. If you look at what stores are doing today, if you look what is happening in the mobile environment, very much they are interconnected, even with stuff like IPTV.

The notion is the digital use of information is growing and these issues go far beyond the traditional Internet.

MR. HOOFNAGLE: I have skipped a slide in there. In our report we argue that individuals when they see the term "privacy policy," they think it means opt in.

It is about time the Federal Trade Commission bring the law in line with that expectation. This is not the result of some intentional action. It is not that businesses have tried to deceive the public.

What has happened is that the very structure of privacy protection in the United States has led people to believe things that are not true. It is detrimental to privacy and ultimately to public policy and the Federal Trade Commission has to address these issues.

If I may say finally in 1996, Beth Givens from the Privacy Rights Clearinghouse recommended the FTC set benchmarks for the formation of whatever policy approach the industry takes. We need benchmarks today and we can't do without benchmarks.

Thank you.

MS. HARRINGTON: Thank you.

(Applause.)

MS. HARRINGTON: I'm going to ask Trevor and Peter or Peter and Trevor in that order for about three minutes of thoughts on what you have heard so

far, and then we will have a more robust discussion.

MR. SWIRE: Thanks. I have reactions.

I will in three minutes try to do three things. How facts and technology are likely to change in the last 10 years, a comment on market failures and a comment on the new Congress and how that changes things.

On facts, I think one of the big changes in the next 10 years is that sensor devices become roughly free, the way computing powers become free. Nobody used to have a camera. Now we all do. The camera is also a tracking device. We are going to have free sensors and the database from these networks of the sensors. That will create a lot of policy challenges.

On market failures, I think Solveig Singleton -- I agree a lot with how the markets can cure many market failures. I wrote an article on eBay called "Trust Trap," and highlighted that.

I think a big job for the FTC to see exactly when it happens and when it doesn't happen. The FTC ought to be one of the expert places at figuring out more or less automatically and where enforcement standards and other things have to happen.

The third thing which clearly wasn't part of

the agenda today but it is too interesting to skip is what changes with the new Congress that we seem to have as of today. A couple points on that.

One of the big questions you think about the next decade is do you think the Democrats will have the House for at least 10 or 12 years which is what happened the last time the House turned over, or is it just two years and a temporary thing.

A lot of people in Washington will try to figure that out. I think there are some reasons to think it might be a fairly long lasting change.

If that does, it changes the boundaries of how policy gets done on a lot of these issues. If we look at Chairman Tim Murrows, he had a nonlegislative agenda, let's do enforcement, let's do rules, but we are not going to do legislation.

The current Commission has rarely been pushed in the privacy and security area by Congress to do specific things.

But I think if you imagine John Dingel chairing the House Energy and Commerce Committee and the history of some of his inclinations, we can see three sorts of changes that might affect how the policy at the FTC gets done with relation to these issues.

The first is oversight. Everyone expects much more active oversight from Congress in the next period, people being hauled in front of the Congress, being asked tough questions, being given subpoenas and not being able to hide. That's going to change and it will force certain answers out into the open.

A second thing that will be a broader set of consumer issues that can get on the agenda. In the last several years, the federal action has happened only after the states acted. Data breach started the states, Spam started the states, spyware legislation started at the states. We might see things start in Congress.

If they start in Congress, that will affect how the FTC is going to be acting because there will be some active people just a few blocks down the road demanding change.

The third thing is when it comes to privacy and security, there has been a real hesitancy over the last five or six years to imagine legislative solutions except in very targeted areas. There will be at least imaginings of new initiatives.

So as the FTC imagines its own next ten years, it might be in a policy environment where there will be a much more sustained set of

conversations with Capitol Hill, and I think a strategy for the FTC should take that into account.

MS. HARRINGTON: Thank you, Peter, right up to the the minute thoughts about what the future may hold.

Trevor.

MR. HUGHES: Thank you. My name is Trevor Hughes, and I am the executive director of the IAPP. We are a professional association that represents people who work in the field of privacy.

And 10 years ago, when the FTC first started looking at privacy issues online, we didn't exist. And the profession of privacy has really emerged over the next decade. And I think we will continue to grow and begin to stand shoulder to shoulder with some of the great professions.

We now boast 3000 members in 23 countries. I think our growth is a reflection of many of the factors that we have been talking about over the last three days.

Let me reference a couple laws that I am sure we have all heard too many times.

Moore's law tells us every 18 months to two years the number of transistors on a silicon chip will double. That has proven to be true since the

co-founder of Intel famously created this law, that our processing power is increasing, almost at an exponential rate.

At the same time, Kreter's law tells us storage density increases at the same rate as Moore's law. In any given amount of storage we can store twice as much in that same amount of space every 18 months. There is also research that shows how precipitously the cost of storage has dropped.

Peter mentioned the ubiquity of IP addresses and data sensors, the ability to gather data. It is very clear that data is moving faster to more places and coming back from more places than ever before and it is being stored in quantities that were unimaginable years ago.

I think now how much storage I just have on a flash drive in my pocket, and that is many thousands times more the amount of memory on my first desktop computer.

When I think of those two laws and I think of the growth of the privacy profession and some of the challenges that we have discussed, I think that I would actually reflect on the issue of the first half of this session, and that is trust.

Jules Politneski, who is on our board and is

the chief privacy officer at AOL, used to be the commissioner of consumer affairs in New York City. He describes the problem of indicators of trust, that in New York City, if you were to go to 8th Avenue and buy something from an electronics shop that had a going out of business sign on the window for the last six months and get a dusty box and a salesman who demanded that you pay in cash and didn't give you a receipt, you had many, many, many indicators of distrust in that transaction, and your expectations of that transaction are probably far less.

You could take that risk, certainly, but certainly it would be much less of a risk to go down the road to a Best Buy or Circuit City where you get a receipt, a warranty, you pay with a credit card.

Jules said and I think he is absolutely right that in emerging media our indicators of trust can't catch up. We see new channels develop on an increasingly fast pace, as Moore's law and Kreter's law give us new processing and powers.

I think one of the great things we need to face in the next Tech-ade is the need for these indicators of trust. Privacy professionals have a big part in that job, and I think they are the guardians of trust for much of the information

economy particularly from a corporate perspective. But we have seen agencies take this up by naming chief privacy officers, DOJ, U.S. Postal Service, many others.

Metcalf's law, as many of you may know, is a law about networks, and it says that the value of a network increases by a factor of the number of nodes in a network.

The proof of that law is that the first person to buy a fax machine was kind of a sucker. They got it home, opened up the box and were unable to do anything with it. It was only when the second person bought a fax machine that that first fax machine had any value whatsoever.

Metcalf's law is right. I would add a layer to it. The value of the network is not created necessarily by the number of factors in the equation, but the value of the network is created by the flow of the data through the nodes in that network.

I would like to suggest to you that privacy professionals, that we in this room, that the FTC need to be the guardians of that value exchange and the information economy.

Thank you.

MS. HARRINGTON: Thank you, Trevor.

(Applause.)

MS. HARRINGTON: We are going to have time for questions from those of who you are here. Let me begin with one.

Helen, I think that you make the point very well that privacy, that is how people feel about their information. Whether they are willing to turn it over or not is a highly nuanced matter. You would say it is a normative matter.

I think at the FTC over the last decade we have come to agree with that, and in fact it is so nuanced that it is very difficult to do hard economic analysis and cost-benefit analyses on that front end.

The one thing that I think that we have focused on and that there is a broad agreement on is that it's extremely important once information has been collected to safeguard it and to ensure that it is handled in a secure fashion.

Going to our trusted source group over here, how important in your view is that promise of information security to being a trusted source? I guess I would invite the whole panel to chime in on that.

We may have a polling question on this in a moment, too, so those of you in the audience pay

attention.

On being a trusted source, where does information security, data security rank in your thinking?

MR. BRENDLER: It ranks -- in the study that I mentioned that we did about indicators, it ranks very highly. Privacy and security ranked very highly as indicators.

MS. HARRINGTON: Are you equating privacy and security?

MR. BRENDLER: No. I'm sort of joining them together. That's the way they were joined together in the results of the research.

On the heels of the presentation we just heard, we also have a lot of research that says consumers say they want privacy policies but they don't really look at them, or when they do, as Chris and Joe mentioned, they are almost impossible to understand. They are written for attorneys.

Consumers don't know what to do with them. But they want them.

MR. SHIPMAN: That is the exact issue. Privacy is in fact much different than security at, least as how we talk about it within eBay. Privacy is the use of information, how it might be shared,

how it is collected, how it is processed.

Security is who has access to that information and how are we protecting it physically, logically.

So naturally, while I think the two must work together and are both equally important, they are distinct. You have to have physical and logical controls that equal your problems, and you have to use information equal to your promise, and that promise is the privacy policy.

MS. HARRINGTON: That's a very nice distinction and an opportunity for a polling question.

So as you go online to do whatever it is that you do, do you care more about privacy? That's number 1. Or the security of your information? That's number 2. Let's vote.

While we are voting, we are going to jump right down the line.

MS. SINGLETON: I think there are some very different types of data handling here, different types of data problems.

One is is someone going to get ahold of your credit card number or Social Security number, and a second question is Spam.

Another question entirely is marketing data, which might be sensitive in the health context which is where the opt-in standard grew out of but not at all sensitive if someone is buying pet food.

I can see Chris is looking puzzled. I can explain that if you want. There are safety issues as well, like is my child trying to talk to someone who is trying to get their address and their real age. There is really context important, context dependent changes here that I think are very important.

MS. HARRINGTON: Thank you. It looks like we have a lot of security hawks today.

Turning back to our privacy group from our trusted source group, what do you think about this distinction that is drawn between privacy and security and the relative importance, and particularly, Peter, let me throw that question to you as someone who has some views about what we ought to be doing.

MR. SWIRE: Well, one way that I draw the distinction is security keeps out unauthorized users. It stops the hackers from getting in and the wrong employee from looking at it.

That's a baseline that pretty much everybody thinks should happen. You say there's a

cost-benefit. You don't put 6000 locks on your doors, but you put on enough locks to make sure to keep the regular threats out.

One reason it is easy to go on B for security is that without having some locks on the door, you can't pretend the house is safe.

Privacy tends to be more a decision about which things we should share, medical or not. That tends to be a much longer discussion. And the whole privacy literature has to do with different chapters of that discussion.

MS. HARRINGTON: And a highly nuanced one. I think in part, Helen, that is a major point you are making.

MS. NISSENBAUM: What I'm trying to do in creating a theory about it is not to say it is so nuanced, let's kind of throw up our hands and say it is too complicated, but that it is nuanced in particular ways and that we can actually get a handle on it and by having a structured way of thinking about it, we might actually be able to come to better decisions, and, again, responding to what Peter has just said, that we might have a better sense of what sort of flows of information are acceptable to people and what are not.

Once we have decided that, then the security question comes in, which is how to then protect it in ways that you have set out in your policies.

MS. HARRINGTON: How do you decide that? Do you apply some sort of cost-benefit analysis at all? What are the objective standards for making those decisions?

MS. NISSENBAUM: Those meaning --

MS. HARRINGTON: The decisions about acceptable levels of information flow.

I'm having a hard time as a lawyer interested in economic analysis as well as fitting this into --

MS. NISSENBAUM: It is a not a cost-benefit analysis. I'm sorry because I tried to squish in a very brief period and maybe I tried to cover too much.

When you look at it in the particular contexts, the one that we know quite a lot about, for example, is health care. We have some good ideas about what the norms should be in a health care context.

So that has to do with protecting -- there are multiple questions to ask when you try to settle on what those norms should be. But they can have to do with protecting people against harm.

But they can also have to do with the actual success of the health enterprise itself because if people don't trust, then they are not going to be willing to share, and that will be bad for health in general and health in particular in individual cases.

MS. HARRINGTON: In the time we have remaining, if there are questions from out here, make yourself known, and we will work you into the discussion.

All right. Trevor, I'm going to turn back to you on this issue of developing some sort of framework for setting norms for privacy flow and data flow, picking up on what Helen was just discussing.

MR. HUGHES: I think the contextual concept of privacy is actually right. I think all of us just inherently understand that privacy is contextual.

Peter and I were trying to figure out who it was that said at a CFP conference that Americans value their privacy but the value is 50 cents off a cheeseburger.

I think that is right in certain contexts. But in other contexts, you may not be willing to give over your zip code because it seems odd at that point in time.

MS. NISSENBAUM: Or even your name.

MR. HUGHES: Indeed, or even your name. There is even more layers than that.

There is certainly the generational layers that we heard discussed earlier, that different generations have different approaches to privacy.

Allen Weston's research has given us another set of slices on the population, telling us that there is really a spectrum of perspectives from privacy fundamentalists to privacy concerns to the big mass in the middle, being privacy pragmatists.

It is an incredibly difficult matrix to wrap any type of standards around, and I think that's one of the reasons that it has been very challenging.

And I apologize, this is self serving. I think it does speak to the need for a profession in the middle of this, that this is a professional job.

It is not just sort of a technocratic response. It is not a compliance response anymore. Privacy professionals are much more than that and they are doing very, very sophisticated things.

MS. HARRINGTON: Joe.

MR. TUROW: Can I add one more complexity to the problem of context, which is real basic. You may think you are giving up bits of information for one reason and what ends up happening is due to the

combination of statistical algorithms, the buying of third-party data, you end up giving up information for purposes you have no idea about, and it happens every day.

So, for example, if anyone goes to a major supermarket, you gave your data when you buy using a frequent shopper card, and virtually -- 80 percent of Americans use frequent shopper cards and for obvious reasons; you get discounts.

If the supermarket has a relationship with Catalina Marketing, for about 102 days they are storing your information, not your name, but your information as a number, like a cookie as to everything you have bought.

The next time you come in, through complex algorithms they decide how much money to take off for any particular product not related to what you are buying now but taking into consideration everything you have bought over the past couple months.

How do you know that the cat food you bought or the dog food you bought on a particular day three weeks ago will affect whether you get cents off on a totally different product or maybe the person in back of you will get cents off on the dog food but you won't because you are an established buyer.

The kind of calculations that have to go into a person's mind-set in everyday shopping behavior become quite complex. And the chagrin that a person might find in the small situation of a person behind that -- and I have had situations like this, how come you have a discount coupon for Pepsi and I don't, or people who go into the test supermarkets where they go through the aisles with shopping buddies in which they give them different prices as they are walking through the aisles.

So the algorithms that go into figuring out what it means to give data are almost impossible to calculate.

MS. HARRINGTON: All right. We have only about three minutes left.

I have one last question that I would like each of you in the remaining three minutes to address, and that is in terms of information and data privacy and security, what 10 years from now do you think we will be dealing with as the greatest concern or issue as we look ahead 10 years? Or five years.

Let's look out beyond now. What will be the greatest concern?

Trevor, we will start with you.

MR. HUGHES: I think that the rapid emergence

of new communications and data flow channels that are inherently open, such as e-mail historically, that as those channels emerge, we can't catch up with standards and friction in those channels quick enough to prevent the fraud and abuse that we see in wide-open channels that lack accountability.

I think the fact is that we will see more channels emerge and that they are going to be increasingly digital based and open and lack the accountability necessary out of the gates for us to have controls of them.

MS. HARRINGTON: Peter.

MR. SWIRE: Something not mentioned today, not the FTC's job, but these private sector amazing collections of data are all available to the government presumptively going forward. They are no more than a subpoena away.

As a democracy, we have to figure out. We don't expect them to be looking at us and how are we going to work that out.

MR. TUROW: I agree with both of those. I would also like to add the increased nichification of society and the electronic overlay of that. You may get a different 60 Minutes from what I get with different commercials because you're valued more by

certain companies than I am or because they tell different stories than I am interested in. What does that do to a society when people are constructed in that way?

MR. HOOFNAGLE: We are going to have ubiquitous identification and tracking through radio frequency ID.

The New York Times recently reported on researchers who got credit cards that are RFID enabled, and these credit cards were reputed to be secure but they were able to waive an RFID reader and identify whose card it was.

We are moving into a world where there is ubiquitous but silent identification and tagging, and we will have to ask ourselves how the notice and choice regime is going to work.

MS. HARRINGTON: Helen.

MS. NISSENBAUM: I think I'm now echoing some comments that were made earlier throughout this event.

Contexts that are important to me in my work, we can think of them as part of the culture that have evolved over hundreds and sometimes thousands of years. If you think about the Hippocratic oath, you know that has been part of the health care context

for centuries.

But the technology that we have just heard about is moving at a pace that is changing the quality of life in ways that we haven't had time to register how this will alter the balance of interests and the balance of power.

I'm afraid that we are going to 10 years from hence or even five years be in situations where we haven't had the opportunity to really evaluate and resist some of these changes because they have disturbed these cultural contexts in ways that have been deleterious to us.

MS. HARRINGTON: Well, thank you. And thank you all, all of you, for a very thoughtful participation.

We are going to have a 15-minute break now. We will resume right at 4:00 for the consumers' perspective.

(Applause.)

(Break and Technology Pavilion.)

MS. SCHWARTZ: I would like to begin this panel.

This is not high tech. We are going to have a conversation with a panel of experts who have been following the hearings, either by the Webcasting, the

blog or in person.

We are asking them to carry out what is probably an impossible task, which is within a very short period of time -- we have roughly an hour -- to have them tell us what they heard and what they take away from these hearings from a consumer perspective.

To begin, so as not to waste any time, I'm going to introduce Jo Reed, who is with AARP, an organization we are all familiar with.

She is the national coordinator for livable communities and consumer issues in the AARP's federal affairs department. She has been with AARP for over 20 years and working as a lobbyist on low-income consumer protection and social services issues.

We have heard during the hearing something about older Americans and to some extent concern that they are not participating in the technological developments.

I will ask you to tell us what you have learned from these hearings and how it affects your group.

MS. REED: First, I want to say how appreciative we are to the FTC for holding these hearings.

I have not been able to personally

participate in observing the hearings myself because of so much going on, but we have people all over AARP plugged in watching the Webcast and feeding in their observations. And they have found it so, so interesting.

It is said often and perceived that older people are not taking full advantage of advancing technology. In the upper reaches of the older population, I'm sure that is probably more true than not.

We actually find in the 65-plus population, we have some of the fastest growing participants in computer use in the entire population. Of course, they are not out there mostly checking out all the shows and purchasing -- shopping for different products. They are using it for e-mail, keeping in touch with their grandchildren and others.

In the process, they are becoming more familiar with the technology. I think it is something that has caused us to look very closely at what is happening in the world of technology and how they may be affected by this.

Many, many interesting points have been made by the speakers during these hearings. One I would focus in on is privacy and security.

Again, even though older persons are mostly using the computer, the Internet for e-mail, increasingly midlife and older people are going to be using it for all kinds of things. So security is going to be an issue for our members who start at age 50 and up.

One thing I know has been talked about, in particular by Fred Cate from the Center for Applied Cybersecurity Research is the erosion of privacy in the public sector which may lead to an increasing risk of exposure of private information in the private sector.

That's something in particular that we have been looking at and are very concerned about. I would point specifically at the Real ID Act which was passed in 2005.

It was part of a Defense appropriations bill and aimed at national security and dealing with immigration issues, but it creates this network of databases that all the states participate in, an interstate network of personal files to create a federally acceptable driver's license which will eventually be required for use for accessing any kind of federal benefit, like Medicare or Social Security.

This database is going to be connecting

federal sources of information with state sources of information. And a breach in that kind of information could lead to breaches in all kinds of private sector data as well.

So we at AARP, among other organizations and states, are looking closely at action to implement that law in the year ahead, regulations that will be written and looking at ways to see how we can protect that data and encourage perhaps even some changes to address that problem.

So I'll stop there.

MS. SCHWARTZ: Thank you, Jo.

Now I turn to Susan Grant, who has been with us 10 years ago when we had our 1995 high-tech global hearings.

MS. GRANT: I was probably warning you about Spam then.

MS. SCHWARTZ: She is vice president for public policy at the National Consumers League. She works in the area of electronic commerce and financial services and is the director of the NCL's National Fraud Information Center and Internet Fraud Watch Group.

MS. GRANT: I have to say I found the presentations and discussions in the last three days

really fascinating. I decided to focus on one particular word that has come up over and over again, and that's the word "control."

We have heard that it is important for consumers to have control and that tech can actually give them more control in some cases, but when we saw the hilarious video about the nagging computer, it reminded me that sometimes technology controls us and not the other way around.

That's not necessarily a bad thing. For instance, I think that we are certainly in favor of secure by design, having security be the default mode when we are using different kinds of technology.

If we do have to take control as consumers, how do we do that? I think it is really difficult.

Most of us aren't technicians or lawyers. We don't want to have to figure out how to navigate complex technology or complex legal agreements about how to use it.

We can't control what we don't see. For instance, how our information is collected, aggregated and used in ways, for instance, to profile us and perhaps offer us a different price than someone else would get for something that might not always be to our benefit.

And we can't control the security of our information when it's not in our own hands, when it is actually in the hands of other people or organizations.

We also lack meaningful control when the terms of using technology are one-sided. And I think we see that with end user license agreements, as was previously alluded to, in privacy notices. We don't understand them, but even if we did, it is really a take it or leave it situation, and we usually want to buy or do whatever it is that we are trying to use the technology for.

One thing that gives consumers real control is their legal rights, and as we have heard, many of the new things that consumers are doing with new technology are not covered by existing laws or there are disparate laws depending on, for instance, which form of a new payment mechanism they are using to pay for something.

I was interested to hear some business representatives say that they wanted more clarity, more certainty about whether what they were doing was within legal bounds.

I think that both consumers and businesses are somewhat hindered in the full use of these new

technologies by the lack of a legal framework for things like privacy and security.

So I think it is time for the Federal Trade Commission to take another look at that and support some sort of framework that these new business models could actually be built upon.

I also think that there is room for more guidelines and best practices, and those can be developed by business organizations, by government, by consumer organizations, by some of us joining together to do them. And I think that would be useful.

I'm going to stop there.

MS. SCHWARTZ: Thank you very much. We should have time at the end for additional dialogue.

Let me turn next to Dawn Rivers Baker. She is the president and CEO of Entrepreneur Publishing and editor and publisher of The MicroEnterprise Journal, which are businesses that employ fewer than five people.

She will tell us more about her work and the people that she is interested in our learning about. They have been below our radar screen, and it is time they saw the light of day. So Dawn.

MS. RIVERS BAKER: Thank you.

Let me give you some background about microbusinesses.

Microbusinesses, as was mentioned, are firms with fewer than five employees. Most of them are nonemployer microbusinesses, they have no employees at all. They constitute 91 percent of the businesses in the country, according to the most recent data that has become available from the Census Bureau, and three out of four U.S. firms are nonemployers, they have no employees.

This group is seriously impacted by everything that comes out of a set of hearings like these. I just this week got some information from Sinal Ghandi of Jupiter Research, who is working on publishing research on the online activities of microbusinesses.

And one of the interesting nuggets of information that she gave me before I left my office to come here was that microbusinesses are uber users of the Internet. They are more active online than normal consumers, they are more active online than the owners of larger small businesses, they are even more active online than larger businesses.

They buy online, they sell online. They participant in social networks. They participant in

listservs, they participant on message boards, they blog, they Podcast, they video blog. They are all over the place.

At the same time, when the FTC brings together industry representatives to address issues like e-mail deliverability, like privacy, like security, microbusinesses are not represented at that table, and that's unfortunate because they operate in ways that are unfamiliar to both the government and to larger corporations.

And because of that, the solutions that are often proposed when the FTC turns to the private sector to solve a problem are solutions that either do not take into account the operational realities of a business that doesn't have an IT staff or doesn't have any staff at all except one person, that the results of those limited resources, or the solution that they come up with winds up being priced out of range of microbusinesses.

One of my favorite examples is around 2000-2001, when privacy was on everybody's lips and the privacy seal programs were started by trusting in the BBB online and they were great, everybody said they were great, but microbusinesses could not use them because they cost too much. We had no way to

authenticate ourselves as trustworthy businesses.

The same thing is happening right now with the e-mail deliverability issue because microbusiness owners by and large don't use dedicated e-mail servers. We use shared hosting plans. So that the e-mail authentication technologies that have been proposed, with the exception of SPF records, those aren't available.

So if we don't want to go with a third-party e-mail service provider, if we want to do our own in-house list work, we cannot get our e-mail authenticated.

And then we wind up getting our e-mail blocked, because one of the interesting things that happens online is when you are a small unbranded business, you can run a squeaky clean outfit and it is still hard for people to trust you. Whereas, if you are Amazon, you can have all kinds of securities breaches and problems but you are Amazon, so it is okay.

That's an issue. I also think that right now there's a possibility that a marketplace that was as close to an even playing field as you are going to get in an imperfect world, and it wasn't really an even playing field to begin with but it was close, is

about to change profoundly.

I'm talking about net neutrality, which is an issue that could have a really, really profound impact on microbusinesses.

If we are talking about a future in which the demand for multimedia content is going to be ever increasing, well, the content is not beyond the microreach. We are already videocasting, already podcasting.

But if the fast lane is going to be reserved for the people who can pay for it and the consumers are going to be trained to not have the patience to wait for the slow stuff to load, then we are going to change from whoever has the best content will win to whoever can pay for the best delivery will win.

Ultimately it is important for the federal government in general and for this agency in particular, I think, to have more of an awareness of the microbusiness segment of the economy, particularly online, because it was the Internet that I think really resulted in the explosion in the number of microbusinesses over the last 10 years.

They are like plankton. They are very small and insignificant, but collectively they are a really, really important part of the economic

ecosystem.

They need a place at the table. That is very important because most of the people in this town have no clue how these businesses operate.

MS. SCHWARTZ: Thank you, Dawn. I have a feeling you are no longer below the radar screen.

I don't know how this happened. I just realized that we have all the women sitting on one side and all the men on the other. This was totally random.

Let me turn next to Beau Brendler, who we just gave him a little break between his last panel and now this panel. As you know, he is director of Consumer Reports WebWatch.

And Beau, you have been attending all of the hearings, you said, and participated in a number of panels perhaps and been thinking about how what you have learned here is going to affect how you do your business going forward. I will give you an opportunity to speak.

MR. BRENDLER: Thank you. Thank you again to the FTC for being in this role at the last panel of these hearings.

To jump right in, I will be a little more notes intensive here than I usually am in panels

because I have been taking a lot of notes.

Like others, I think I would have to say that this set of hearings has been about, with a few exceptions, privacy and security, two different concepts, as we talked about, and in certain circumstances not necessarily completely separate, I think, but that's certainly something that can be talked about. I think a key word is the term consent.

I think a major part of what affected me in thinking about this was a bit of a dialogue yesterday between Brian Wieser of MagnaGlobal and Jennifer Barrett of Axciom.

Brian said that a majority of Americans are concerned about their privacy and want to control it, advertisers are worried about going over some undefined line and creating backlash.

Later on in the discussion Jennifer said consumers want choice, but they want choice they can understand.

I want to talk about that just a bit. In October 2005 Watch published a national survey again, and we found that 30 percent of Americans have changed their Internet behavior, defined as buying less stuff, using Internet less, even ceasing its use

because they were concerned about its negatives, its dark side, other factors.

I'm not going to go as far as to say that's a backlash. But we need to remind ourselves that consumers -- I don't mean to take away anything from them here -- sometimes don't understand this online world as we do.

I want to cite a Privacy International study that was released Thursday of last week ranking 36 countries in terms of privacy. This also includes surveillance. In terms of statutory protection, the U.S. is the worst ranking country in the democratic world in terms of the health of national privacy protection.

Last week U.S. PIRG and the Center for Digital Democracy wrote a legal finding to the FTC. I have a copy of it here. I would like to enter it into the proceedings. It states that it is matter of time before intensive behavioral tracking data gets mixed with other personally identifiable information.

There was some discussion of that yesterday. You can read this. I won't go into it here because it is pretty long. It is about 60 pages long. It is about privacy.

So what to do or what to sort of consider.

I'm not sure business best practices and guidelines appear to me as consumer concerns here. Every site has a privacy policy. I'm not sure how useful they are to people at this point.

Privacy policies are full of legalese spread across several different places on the site. Someone yesterday cited the NAI guidelines specifically pertaining to advertising and privacy.

I have a fair amount of expertise in this arena, and I never really heard of the NAI. I don't think they have a lot of resonance with consumers. Last night looking at that as a journalist, if I were to look at them, I would characterize them as something of an industry group, perhaps as an industry lobby group, and I don't necessarily think they would pass the sniff test with consumers.

I would invite them to get in touch with consumer organizations and bring them into the mix when they are creating guidelines for their own industry.

Just to mention briefly at the end of this bit about privacy, we did a project for Consumer Reports magazine about dating sites, and I want to sum up some of the things I said by something that is buried very deep in the privacy policy of Americans

Singles. "You should not expect and we do not guarantee that your private information will always remain private."

Is that good or is that bad? If I read that, are they being honest in disclosing or is that good? It is buried in the middle of the privacy policy.

So what to do? A few people over the course of this have mentioned fines. Maybe there should be fines in situations -- this crosses over into security, but when there is a major breach of data, maybe there should be some more severe recriminations than there are.

We have some concerns that guidelines in the arena of privacy and security create a low bar for minimum compliance rather than encouraging them to do something really creative and interesting.

We heard that 30 states have breach laws. There is a notification issue. I'm not an attorney, but if 30 states have breach laws, you saw what happened with the credit card industry. A lot of them relocated to Delaware and South Dakota because of the laws there.

Many consumers still believe the number one privacy risk is someone intercepting your credit card data in the middle of a transaction. Probably not

something anybody here worries about.

Many don't realize the greatest risk is when the data gets warehoused by an irresponsible third party. So let's think about a campaign to compel businesses to only contract with data storage companies that have a best practices pledge in place.

I will try to speed up here.

A number 2 concern, privacy and security was the major theme. The next one is consumer education I think to some degree is failing. Consumers are besieged by choices. 21 percent of consumers don't even have security software installed in their home PCs.

At the same time this is happening, fraud is increasing, I think, although I did hear some numbers today I believe from a gentleman from Experian who said that's not necessarily the case, or at least with identity theft. I don't know about those numbers from my perspective.

Identity theft is increasing. The burden of correction falls on the consumer.

I will skip forward a little bit and say something about search emerged within the last three days as sort of a critical point of beginning for everyone, whether they are searching for information

on the Web or searching the Web.

I think consumers have a difficult time distinguishing among paid placement and organic search results.

In 2002, we did a study that said 60 percent of the population doesn't even know that search engines take money to order results. The number improved slightly to 57 percent of the American population don't understand the business model of search engines. They are more like the Yellow Pages than objective oracles of information, I think.

And I mentioned early in the panel that I would get back to CourtRecords.org, a site I mentioned earlier that's fraudulent, how does it relate to this. CourtRecords.org is number one or two in page searches on Google if you type in the words "background check."

And in Google's paid listing you will see a document that says "consumer's guide to background check sites." You click on that and you get a page, I don't know who built or generated it, but one of the sites named is CourtRecords.org. It is a fraudulent site.

So consumer education I think to some extent is being grabbed on to by people who probably should

not be educating the consumers in the way that they are.

Very quickly, things that were not talked about but were mentioned over the course of the past three days, SCO and SCM, searching and optimization. Booming, terrific, but a large amount of unregulated and unmonitored business will lead to a situation where the best-optimized sites and those better at playing the system get higher placement and higher ranking.

Finally, it was just alluded to but not much has been discussed about trustmarks. I bring them up here to say basically I don't think they have had a lot of resonance in the trustmark realm in order to address some of these issues.

And just quickly, out of a sense of irony, as I was walking over here this morning I looked at the business section of USA Today, and the lead story says "If it is really you, what color is your car? A growing number of banks and retailers are moving beyond Social Security numbers to verify your ID. They are relying on such personal details as your car color, your father-in-law's name and the city you lived in five years ago. No, never gave them this information. They pulled it from public and private

data. Private details are increasingly being used to," et cetera, et cetera.

I won't bore you by reading through it. There it is, and I will stop there.

MS. SCHWARTZ: Thank you. I want to turn next to Brent Embrey, who is the director of the telephone privacy unit of the Indiana Attorney General's Office.

And as a law enforcer, we have heard over the last few days about the stress that all of these developments are going to put on law enforcement. So maybe you can speak to that.

MR. EMBREY: I guess I should give you one perspective. My job in the consumer protection division, where we get 11,000 complaints a year, is to figure out what to do when things go wrong.

So if I sound like I might be coming from the opposite angle, I do understand that we deal with the cleanup angle of it.

It is very beneficial to have a conversation in advance about what steps can be taken in terms of best practices within the industry in particular to try to stop some of these things from happening.

I can tell you from my experience we see a lot that involve online transactions and security

breaches. That's what we are dealing with.

I would point out, to state the positive, when you step back, as much as we get these consumer complaints, I have never seen the real numbers, but there are millions and millions of transactions that happen every day without incident, which gives me some confidence that something is working well.

The natural flip side to that is that fraud is very easy with a computer. If you watched the movie Catch Me If You Can and saw how he went through the steps to create these identities and you listen to that man Frank Abenal interviewed today, he will tell you it is much easier to do today what he did back in the early '70s.

It just cuts both ways. We have a lot more choices available, but a lot more pitfalls we have to watch for.

I would reinforce after listening to this and from my own experience, the question for the next 10 years is who can you trust online. That's the question. I almost feel like being an interloper in the last conversation, because I think that is really thematically where the industry and all the concerned parties need to be.

I believe it is an opportunity for market

participants, quite frankly, to provide some great consumer protections purely motivated by the market, on the one hand, and if they do that, a great opportunity for them based on their using best practices in a variety of areas to make a pretty good business for themselves, providing the good consumer protections in their own online transactions.

In order to do that, they will have to differentiate themselves in the way they handle the privacy issues. I don't mean legally written privacy statements but a privacy commitment that the information that we as a company take from you is going to stay with us and will be used only for the purposes of servicing you, and they will have to be the best they can at the security best practices which are continually evolving.

They will have to have a very intense customer focus and essentially guarantee they will have a successful transaction on their system in order to satisfy those customers. And then, of course, things do go wrong sometimes, and if they do, they have to be completely candid with their customers as soon as they possibly can.

Even if you do experience a security breach, something you couldn't possibly control, you need to

let your clients know as soon as you can.

Rather than hearing two months later that you had a breach, they would appreciate knowing within a week and that you made the effort to apprise them of the situation, let them know what the odds are something could happen, and then you can move on from there and I suspect save a lot of faith with your customers.

The rest that don't go that approach, my opinion from where I sit in Indiana looking at my consumer complaints I'm getting, the rest of them are on a collision course with the public.

I don't think the public is anywhere close to being aware of how much of their information is captured, what is done with it and how many people are able to touch it, either electronically or physically if they want to print it out.

The issue is either going to be forced by the government or forced by the public at some point. As you have watched this Internet monster evolve, it has regulated itself pretty well.

I would hope that the market gets itself to that point before you have a huge public backlash. People are just not aware.

I don't think if they watched this on TV that

the audience will get particularly big, but it will be a big issue at some point.

I would suggest to you also, if we were having this conversation about the next Tech-ade in 2016, that there are probably companies that will have been able to establish brand loyalty based entirely on their trustworthiness in the Internet marketplace.

I think that's a very effective tool for them. It is good business sense and helps consumers. Our perspective in Indiana has always been try to create a win-win situation. We want to find ways to craft some solutions.

A couple of brief issues -- are we okay on time?

MS. SCHWARTZ: Yes.

MR. EMBREY: It is a serious issue for consumers in the next Tech-ade to figure out how to engage the government when they have a problem with some of these technologically related problems.

One are your standard Internet transactions. If there are transactions that are occurring in the United States, I think the attorneys general as a group have done a good job of committing to policing their own backyards.

We have had many, many cases that we have sued online sellers, either via an eBay system or some other electronic transaction who failed to deliver, didn't do a good job or provided a bad product. And even though there weren't any Indiana consumers involved, that was our backyard and we were going to be the ones to take care of that.

Likewise, there might be Indiana consumers who get the benefit of Elliott Berg's work in Vermont who do not live in Vermont.

But in the next decade, the international, the global nature of our economy will make us look to see if there are other options about how we handle these kind of online transactions when they cross the international boards.

We don't have too many options right now. We do see complaints that involve Canada and involve India and, of course, Nigeria. How can you miss that one? That is probably a lost cause. We see a lot from the Caribbean too.

There might be a point where the states and the federal government need to be together and see if there are provisions and treaties that allow us to give some of our laws effect. We are completely unqualified at the state level to do something like

that.

Don't forget your old friend, the telephone. Because voice over Internet protocol is here and it is growing. One of the best fraud-reduction programs there is actually is the do not call program.

Indiana has a very aggressive one. That also has to do with auto dialers and telemarketing fraud. In that case it is all about the telephone records and consumers being the one to actually step up and help us with that.

We have two people who do nothing all day except connect the dots and try to get that stuff through phone records. In our auto dialer statute, the day after Election Day, we have an auto dialer statute that applies to political calls and after warning everybody, we decided we wanted to make sure everybody is on notice.

We were going to force this law in a couple of hot races in southern Indiana, and 527 organizations, which I'm assuming people out here understand, were very surprised when we were able to figure out who they were and haul them into court with phone records and the consumers who got recorded messages and get them enjoined.

(Applause.)

We were bipartisan. One was advocating for the Republicans and the other was advocating for the Democrats.

It is very strict attention to detail if you want to get at some of these technological issues as a law enforcer. I don't think the consumers quite understand how long it takes to try to identify who may have defrauded you on the telephone.

Finally, identity theft, there will have to be a better efforts with the federal state and local people together. I think I have gone over my time.

You have people that have their identity stolen but then somebody comes back a year later and opens new accounts and there is nowhere for them to go. We will have to do something about that.

MS. SCHWARTZ: Thank you so much.

The clean-up matter for this panel is Jerry Berman. Jerry Baron is my former law dean at the law school.

He is president and founder of the Center for Democracy and Technology, working to promote democracy in the digital age.

So, Jerry, it is your time on.

MR. BERMAN: First of all, I want to commend the FTC for holding this very important set of

hearings.

I also had the benefit of being here 10 years ago for that hearing. At that point it raised some issues for me, and I have heard a lot of discussion about some very critical Internet issues.

We raised those issues in a narrow-band context 10 years ago. Now we are in a broadband and digital convergence era, where there is not just privacy but issues raised of whether we are going to have an open and nondiscriminatory platform where everyone can reach everyone and where users have control over content.

That has been the glory of the Internet, and we want to ensure it going forward. That is an unresolved policy issue before our Congress, before the FTC and the special groups. It ought to be considered in much more depth.

There was a whole panel on digital rights management. There is a laundry list on is digital rights management restrictive, is it collecting information. It was issue spotting.

But are we here issue spotting or trying to set an agenda where, for example, the Federal Trade Commission can play the role of trying to make sense for the consumer, which is not just simply holding an

overview set of hearings like this but saying, okay, let's drill down on digital rights management and notice the transparency and interoperability, let's, as Cliff Nagel said, set some benchmarks and bring industry and consumer groups together and have a dialogue and go in depth into these issues, explore technology solutions, explore self-regulatory solutions and say do we need legislation.

But let's say what are you going to do about this problem, set some benchmarks and come back in a year and go at it again.

That continuity and follow-through, whether it is dealing with spyware or digital rights management or net neutrality or an open net, that kind of convening is a critical role that the FTC has played in other contexts and which it can play here.

It is a very different context than saying let's take our issue to the Hill where we can have adversarial hearings and score points and just talk at each other or file complaints before the FTC.

Which brings me to the kind of deja vu. Let's say you could set an agenda and deal with some of these hard issues of an open platform and digital rights management and how do you protect copyright and whether we are heading for authentication at one

end and a national ID card at the other end.

In the privacy area, this is where to me it is deja vu all over again. That's where we started 10 years ago. The FTC has played an incredible role.

They were the first to start discussions. Christine Varney convened people, said what are the issues. There were surveys, privacy guidelines, studies every year, more discussions with Chairman Katofski.

I think that over a period of time, as companies became comfortable with their self-regulatory regimes out there, there has been a growing sense that consumer trust is not going to work with that alone and that we have now come to the point where having a discussion that there are a lot of privacy problems, we are beyond that.

It is already really ripe for Congressional action. It nearly started last year, industry and consumer groups all up there trying to get bipartisan legislation.

I don't think the petition on privacy that my sister organization filed under the FTC -- the forum there is Congress because we have reached a point where we think we know what we mean by notice, what we mean by consent. We know that we need some very

simple short-form notice so that consumers know what a privacy policy means and can use it and trust it and know what a trust band is.

And that trustee has done some great work, but we need to socialize that and find ways to do it because people, consumers on the net do not know who to trust. That has to be solved by I think overarching legislation.

So yes, there's a big -- if you want to add to a privacy agenda, then you would say the privacy agenda is not the data privacy issue. We have some ideas where that should go.

We have a very serious issue with communications privacy. In 1986, Congress passed the Electronic Communications Privacy Act which deals with e-mail privacy and cell phone privacy.

That law is absolutely out of date. It does not deal with stored communications, e-mail stored with Google, has no protection against government access.

There are inadequate rules to protect against government surveillance and access and data mining of enormous amounts of commercial data on the net. There are no rules for location privacy, sensor privacy, all of those new technologies that Peter

held up the device. They are out of date.

The law was passed before the Internet era and before convergence. If you want to start a new discussion there, start it.

I think a series of rich interactive hearings and debates that brought together the different sectors on an ongoing basis with some follow-up would be a very important contribution.

We do not have a federal Internet commission. We don't want one.

We also have problems with engaging our European counterparts and Asian counterparts. We have some serious global issues.

There has been over the last six years -- and I don't want to talk about administration -- a lack of a forum, a summit that convenes the Internet community to say do we share a vision of an open, healthy Internet and if we do, how do we work together on that. And put aside whether we are public interest principle people or whether we are out for widgets.

Somewhere in between we all benefit from a healthy Internet. We need to work together on that.

The FTC is a great forum for that. I don't know how to think more systematically over how to do

that in time.

MS. SCHWARTZ: Excellent.

Does anybody want to respond to that? You set the agenda for the FTC. It has been the agency that has been a convener agency and I think prided itself on independence and being able to convene various groups and sit around the table and work at issues like this.

Putting it into the plate of the FTC is consistent with its history.

One of the things that I heard during the week was a sense, perhaps coming more from business, but I heard this theme repeated -- and I remember it from '95 as well -- that this technology makes the consumer king, they are in control, they can access what they want when they want it.

They put content on the Internet. In other words, it is very empowering. But then I listened to what everyone is saying here and I get a very different sense, that consumers don't know what the rules are, that much is hidden from them, they have concerns about how the Internet and other technologies are working.

Susan, your comment is all about that. We have these two conflicting images about these

technologies and where consumers see it.

MS. GRANT: Where consumers have been most empowered is in spaces that have been least sensored like putting their videos on YouTube. There will be efforts now to commercialize what isn't heavily commercialized, to even offer people services for free that they currently have to pay for in exchange for having to be bombarded with different kinds of commercial messages.

You could argue whether or not that's a good bargain for consumers. There may not be much choice. So in the end, saying that this is something that consumers can consent to or not is kind of a specious argument when this is the way that all of these Web sites are and all of these businesses operate.

I think that businesses have to step back and really think about what consumers want. One business person during the session said that sometimes we try things and we don't know whether consumers will like them or not but we put something out there and that's fine.

I imagine that's how a lot of business works because even though you do market studies and so on, you can't tell for sure what is going to catch fire until it actually gets out there. Sometimes people

will take something and use it in a way that you didn't anticipate.

But to say that consumers have as much control, as has been alluded to during these hearings, I think is not really true and there's no reason, actually, why the Internet should be any different than any other form of media in terms of how it is used to persuade them and market to them. That's the main thing.

MS. SCHWARTZ: Jerry, do you have anything?

MR. BERMAN: The difference between this media versus other electronic media is no one has had to ask permission to connect. Everyone can put an application up there, whether you are YouTube or Google or CDT.

That has been the democratizing piece of it. You do not go to the cable operator and say can I put my show on tonight. That is a very important issue.

Commercialization of the Internet is a different issue. The complaint by the Center for Digital Democracy raises the issue of overcommercialization. But as John Stewart said when they took his copyrighted materials, "if they don't sell enough beer, there is no John Stewart."

It is a money-making venture, and the

alternatives being posed by the public interest community is better business, we sell to each other. It is also some form of -- there is no free lunch for the Internet connection.

I must point out that while I hate commercialization a lot and don't like the pop-ups, it was the commercialization of the Internet, the allowing of commercial traffic over what was once a research network in 1992 that has created this cornucopia of content and an explosion of creativity.

Before that, it was a closed network run for research industries. It was commercialization and allowing commercial traffic that is creating the Internet that we have today.

MS. SCHWARTZ: Dawn, you want to comment and then Jo.

MS. RIVERS BAKER: I think in the context of the empowered consumer, this is an area where it is really important to sort of emphasize the difference between the operational realities of the companies that the FTC has heard from since the beginning of these hearings and the way that microbusinesses operate, because there's a really very fine line between microbusiness owners and consumers.

They have consumer sensibilities about a lot

of issues. So that for the most part, microbusinesses don't do data mining. They don't collect data. In fact, they don't want to know about their customers. They don't want the onerous responsibility about having to safely store somebody else's data.

They would rather not have to do that at all. Their privacy policies tend to be one-line statements that say we don't tell anybody anything about you no matter what, so that there aren't sentences buried deep in privacy policies that essentially say this privacy policy is useless.

Those are some of the things that microbusinesses tend to do that come from that consumer sensibility, where they themselves, not as business owners but as consumers, think about how much spying is possible when you go around online, and they say I can and they say I don't want to do that.

The other thing about microbusinesses that differentiates them from the larger businesses that control so much of the Internet is that they have been baffling economists for a long time because microbusiness owners make decisions about their businesses for reason that have nothing to do with

maximizing their profits.

And because of that, in countless little communities all over the Web, they discuss these issues from ethical points of view and they talk about how can we differentiate ourselves so that they know we might make more money if we did that but we aren't going to do that because we need you to trust us because we don't have eBay's marketing budget. So we need to learn how to develop relationships with you.

I don't know if this is still the case. Back in 2002, Forrester Research found these bitty businesses had snagged a third of the retail market operating like this. They have things to say. They need to be included in the conversation.

MS. SCHWARTZ: Jo.

MS. REED: Yes, from a slightly different perspective. When it comes to people age 50 to 65, the way they use technology tends to be similar to the general population.

Over 65 there is a difference. There is a slower coming to comfort and ease with using advanced technology.

We feel that it is very important that transition systems be put in place to allow people to

come to this and the necessary uses of technology at a pace that they are comfortable with.

For instance, many times people are starting to notice that they can't get access to their wireless phone bill, the specific lines that show which phone numbers they called unless they access it by the Internet.

Well, folks may be using it for writing to their grandkids, but they are not comfortable going in there and don't feel they should be required to do that.

Likewise, the Securities and Exchange Commission is now looking at doing a lot of communication over the Internet, proxy voting, things like that. A lot of voter people who are investors want to continue to have access to it by paper. There are cost efficiencies in going to the electronic medium.

But our feeling is that these kinds of new systems have to be built with the provision of choice to people who aren't ready to go there yet, allow them to enter that world at their own pace.

I just wanted to mention also about disclosures. Disclosures I think Chairman Majoras made the point that hidden disclosures online put in

someplace are difficult to make good use of as they are in the paper format, and that's right.

In general, we think that disclosures need to be tested by consumers, including older persons, for whether they really get what was intended there. A lot of times the lawyers figure it out and they are quite certain this is exactly what will protect us under the law. Whether the consumer has any clue of what is intended or not is another matter.

Whether it is hidden or in actual type that an older person's eyes can read, it needs to be written in such a way that the consumer can understand the intent.

MR. BERMAN: The legislation bandied about the Hill was proposing a short notice system which would allow the FTC to choose the technology and the way to do that.

In other words, so that maybe it is icon driven and you click it, and whenever you disclose personal information, it really tells you. And then it has a short like your calorie counter or -- what do you call it -- nutrition label that would make sense to people and be easy to learn, not that I am not confused by all the different labeling.

But still that there has to be ways to

simplify it for the consumer. Because right now I think I'm an Internet expert. I'm absolutely confused and I click through most of these things. I don't read them. I can't understand them. They are written by lawyers for lawyers.

MS. SCHWARTZ: This kind of consumer choice just deals with a very small part of the whole privacy problem. There is so much that you have no control over. There is no interaction between you and the person --

MR. BERMAN: We talk about this notice choice transparency in a privacy context when it really is a much larger consumer issue across a number of things. You want to know, you want transparency notice and consent and choice about what you are buying when you buy an iPod, and you want the same thing when you are dealing with disclosing personal information.

We need a set of fair consumer practices that apply to net transactions, not just -- and it is bigger than a privacy issue.

MR. BRENDLER: I also heard a lot during the last couple days about the evolution of mobile and maybe cell phones are really going to surpass, they will be better than PCs and this, that and the other thing.

What I am concerned about is there is a lot of talk about the marketability of local information. In other words, I'm walking downtown, I have my cell phone, I want to find out if there are restaurants nearby.

What I hope the FTC would do as that technology further develops is try to be aware of places where trust is sort of taken out of the equation for the consumer.

By that I mean I have my cell phone, I'm looking for a place to eat and what I'm getting on there is something somebody has paid to put there as opposed to a legitimate look at the nearby restaurants.

There are a lot of good actors in the search engine world. Google is very good at labeling. But at the local level, where you see city search and local restaurant search, there is a lot of pay-to-play material that is not disclosed to them as that.

That's also an opportunity for other things to appear in that domain I think that consumers won't even necessarily know what choices they are making.

MS. SCHWARTZ: I hear the chimes. And being a GW law professor, I know that means it is actually

5:00, unless they are a little bit ahead. I think I would like to draw this to a conclusion.

I was very much involved in the 1995 FTC high-tech global hearings. I think this is building on those hearings and that we are looking at a very much changed marketplace but not that much of a surprise, really, of how the developments have occurred since 1995 until where we are today.

I think the Commission has done a wonderful job and Katie Harrington-McBride in putting this together to really bring people of various expertise and experience and perspective to start I think what is going to be a continuing dialogue about what the challenges are ahead.

I thank you all, participants, for coming today and sharing with the group.

(Applause.)

MS. HARRINGTON-MCBRIDE: Well, good afternoon.

I am delighted to see, although I have to squint to do it, so many of you still in the audience hanging on until the last.

We have had such a wonderful experience, those of us at the FTC who worked on the planning committee for the Tech-ade hearings. It was hard

work, but we really enjoyed the interplay between those of us on the working group. And we so appreciate your participation in this event.

(Applause.)

You guys are good. I don't even have to tell you to give yourselves a hand.

We are now to the point where we are going to have some concluding remarks. I am so delighted to have with us the director of the Bureau of Consumer Protection at the FTC and also joining us from the European Commission, Mr. Tamas Andres Molnar.

And we will have a short moderated discussion. We would also like to hear from you. In so many of the panels, we have been going at a full tilt and haven't been able to answer your questions in realtime.

We have kept them and are going to try to blog them in the coming weeks. This is an opportunity for you if you have questions for our panelists to put those cards up in the air, and we will have one of our question card takers come and take it to me and we will try to incorporate you in this closing dialogue.

With that said, let me turn to my panelists and to welcome you both. Thank you for agreeing to

do this. It is a great way to close out this event to hear from you, consumer protection officials from the EU and the U.S., to get your perspectives.

One of the things I heard was a lot will be changing in the next 10 years, everything from whether our beds can record our respirations to how we pay for things, perhaps using our thumbs, to how we draw content off the Internet and what we watch it from.

There are a lot of changes coming. Have you had an opportunity to distill out what will be the major challenges that face consumer protection officials going forward? Lydia?

MS. PARNES: These are just a few initial thoughts.

We heard so much in the past three days. But the first thought is that we have heard from experts from throughout the world about the tremendous changes that we will see in technology over the next Tech-ade, and the changes are incredibly exciting.

But almost every panel has sounded an alert about the consumer protection issues that will confront us.

The first thing is, for those of you who work at the FTC, you won't be out of a job. We will still

be in business in the next Tech-ade.

I think the second thing that struck me is how important consumer education will continue to be.

We have heard that consumers are changing, they are not the passive recipients of ads anymore. They create content. And they become very sophisticated users.

That's really true for some consumers. But some consumers are really overwhelmed by new technology. They don't know how to use it. Or maybe they are scared about the risks associated with new technology.

And, frankly, we heard from some people that there are some consumers who simply can't afford new technology, they are priced out of it. For all of those people, we are going to need to be crafting consumer education messages, and I think one thing is that it is more complicated, that the new technologies will make those messages even more complicated to craft.

And I think just quickly, the final thing that struck me is how fitting it is that we are sitting here together closing out the dialogue today.

Consumer protection is international. There is no doubt about it. It was one of the principles

that we defined in the 1996 report, and I just have to note that Teresa Schwartz, who was up here moderating the panel that you just saw, very modestly said that she had a hand in those hearings.

Teresa, if you are back in the green room and listening to this, don't blush, but she really was the principal architect of the hearings and the very elegant report that the Commission issued after those hearings.

But a principle that was established there is that consumer protection is international. And we have seen that play out over the past 10 years. And we know that it will continue to play out over the next.

So those are just some kind of quick observations.

MS. HARRINGTON-MCBRIDE: That distills a lot of the essence out of what we heard.

What are your thoughts about the primary challenges facing us as consumer protection regulators?

MR. MOLNAR: Fist of all, I will say it was very interesting to listen to the ideas and the problems from the point of view that the same discussions could have been done in Europe, in

Brussels as well.

So it is really underlying what Ms. Parnes just said, that we have international issues. I cannot speak anymore about national problems because of the globalization because of the Internet.

Whenever we have goodwill or bad will behind an action, it can be coming from your country, my country or from a third country. So we have to work together.

Over the next 10 years, to be honest, when I get first the invitation, I got a feeling, very, oh, gosh, the Americans are again ahead of Europe because we are building only a seven-year plan.

But after being here today, there was a question when the moderator asked the people, the members of the panel how do you see the future in a 10-year time, and they seemed puzzled. It was okay in the next five years.

So then I felt okay. We are on the right pace. But a few words, seriously.

It is a very good timing for me because in Europe, the European Commission is just putting together a strategy for the next seven years. 2007-2013.

I have a very good background knowledge about

that, what we want to concentrate on and what are the major issues.

I need to say that the first two has already been mentioned right now. So priority one probably for the EU is the capacity building. And under capacity building, we understand not only information to the customers or the consumers, because it is important but it is just not enough.

We will provide online education. It is available on the Web site and anyone can go there, and since Europe is multilingual, it is available in 20 languages. Even the content is different, expressing the international differences of education and anything else.

MS. HARRINGTON-MCBRIDE: We were talking in the green room about the extraordinary challenges of bringing together so many member nations in the European Union, and the challenges just of language alone are daunting. It puts in perspective our three-day effort here.

MR. MOLNAR: Speaking about capacity building, in the second place I would mention the consumer organizations because we understand it is very important that the consumer organizations should have more active role. They should understand more

the business they are involved in.

The European Commission would like to provide that help to them. It is a shift to what the knowledge base is from the financial support.

So we will try to increase the knowledge, what they have.

And the capacity building, it concerns also the member states and the European Commission. We want to understand better what is going on, what are the major issues, what are the policy issues, where we should concentrate and where we should act on.

We are really concentrating on these points. The second priority is it has already been mentioned also. This is enforcement.

We say that we live in a liabilized life. Every company has the right to do whatever they want. As long as they follow the rules, they are free to do that.

But then we need to give some incentive to those who really do that. And we should try to enforce the others to obey the law. So we say that okay, you can do whatever you want, but we want to make real enforcementment, we want to check that you are really following the rules.

It is not that easy because in Europe, we

have different challenges. The European Commission doesn't have -- at least in this field we don't have enforcement power. So the enforcement is actually on a national level.

So we can only encourage the member states to make the enforcement more efficient.

And the third one is a very hot topic. I think this is part of that already. This is networking. Since there are so many of us already in Europe, we understand how important, how difficult it is to cooperate with others.

It is difficult to cooperate between consumer organizations, difficult to cooperate between the member states, the competent authorities and difficult to cooperate on international level with third countries.

Therefore, we want to give special weight to this one and we will concentrate in these three areas.

MS. HARRINGTON-MCBRIDE: I think that is very exciting to hear. There were some in the audience who attended the international breakfast, and at that breakfast Mr. Bill Kovacic made some very erudite remarks, but he referenced an old and dear friend Professor Louie Sone, who recently passed away and

who is one of the lead figures in the post-war world.

Professor Sone developed a paradigm where he thought nations needed to go in terms of cooperation. One of the points I took away from Commissioner Kovacic's remarks, he noted there needed to be conveners, folks who in the international community will set up opportunities for networking, because it is so difficult in the context of performing our duties on a daily basis to take the time even to properly network with our own colleagues.

That's one of the reasons why this is such an exciting and fun project, to know we would have the opportunity at the end of the day to spend tomorrow talking with our colleagues about what are the takeaways and what do we need to do going forward.

That networking piece will be stepped up a bit as a result of our efforts here.

Lydia, something you said about consumer education puts me in mind to ask a question as we have had as we have begun to do our research on this. There are some challenges because we have so many different audiences and some striation in terms of economics and people's willingness to engage with technology.

I think there are some real challenges, but I

wonder if that can present us with some real opportunities to be there at the teachable moment, to maybe use the technology in a way that allows us to help consumers make good decisions.

I'm put in mind of Bongo, the monkey, here in thinking about how persuasion technologies might become helpful to law enforcement as we help people to make good choices in the online world.

Do you have any thoughts about that?

MS. PARNES: Absolutely. I think that is so true.

As you know, we have a consumer and business education group that has really educated us at the Commission about the teachable moment and kind of finding that opportunity to really get the word out to consumers. I think they have done that very effectively already with some of the online educational materials that are up there.

Carolyn Shanoff mentioned EnGuard Online. It is terrific, just terrific modules. For those of you who are listening to this on the Webcast, if you are still with us, you are sitting in front of your computers, I would encourage you to go look at EnGuard Online if you haven't seen it already.

I think we can use technology to do that. I

think reaching the youngest consumers is really important as we look ahead. We heard about how the age you are really affects how you see the world.

And I think that we will be looking at that as well, kind of figuring out how we can reach kids to really educate them early on about consumer protection issues. And I think for this generation, consumer protection issues are technology issues.

MS. HARRINGTON-MCBRIDE: I think that's right.

Tamas, do you have any thoughts about the use of technology in consumer education?

It sounds like your Web site utilizes technology in terms of translation and providing diverse materials to diverse groups. Are there any plans to try to harness technology to get a consumer protection message out?

MR. MOLNAR: Yes. This is one of the major projects which I already mentioned. Besides that, especially because the EU is continuously growing, I'm also myself one of the countries that joined the EU quite recently, in 2004.

We are carrying out information campaigns for consumers in these countries about the rights, what rights they have, what are the basic messages, what

they should be aware of, what the EU provides them, what are the benefits of cross-border purchasing because people have taught us on it.

Otherwise, they will not be able to use the best use of that.

However, there is big challenge there because certain studies in the EU showed that it is not enough to create the message. 15 to 20 percent of the population in Europe literally is not able to understand the text, what they read. 15 to 20 percent of the rest, 80 percent, is not able to analyze the data.

So if you tell them a mathematic model, it is not good enough. In my country there is an advertisement on the television providing small amounts, loans, and since the law requires them to put down the interest rate, they put it with big letters and they say that "easy access interest rate 250 to 360 percent per year." This is the advertisement.

So as long as such kind of advertisement is admissible at the national commercial channel, you cannot go any further explaining any more complicated issues. These are issues which we need to concentrate on, what is the message, what are the

targeted groups, how they can consume or digest the information, what you want to pass over.

MS. HARRINGTON-MCBRIDE: There are a lot of challenges in terms of leveling the playing field and getting a common understanding.

I think that Lydia, you mentioned starting at the earliest ages and reaching out to consumers so that it becomes a fundamental part of their education. I think that's an exciting idea.

One of the things you talked about is the idea of collaboration. I don't think there is anyone in the room in law enforcement or not who would disagree with the proposition for law enforcers and policy makers around the world to collaborate.

What, though, are some of the stumbling blocks that we have run up against and what are some of the ideas going forward for maybe smoothing the waters and ensuring in the next 10 years our collaboration can be even more effective?

MS. PARNES: Would you like me to go first on that?

It's an excellent question. I think that some of the stumbling blocks that we faced maybe five, six, seven years ago, the biggest one is just that we hadn't worked together. And I think it's --

and that may be going back longer. It could be going back more like 10 years.

I think the fact that bringing in collaborative law enforcement was just, to coin a term, foreign to us.

And I think that once we have done this and we have seen that we can take steps and have successes, I think we have on both sides been very encouraged and we have had a lot of successes. I think we will continue.

Do you think that there have been really specific challenges that we still face?

MR. MOLNAR: I think we have -- if I come back to this idea of networking on an international level, probably this is one of the points where we have very good chances to improve.

Today, earlier some members of the panel, previous panels here, they already mentioned that technology improves so fast that we are not able to anticipate it in advance. We can probably only follow it. But how fast we follow it, this is the question.

So in Europe, we try to put together enforcement alternatives. We created a network and they have to provide help to each other if it is

requested. They have to cooperate.

So it is not a service. This is not some gesture to you. This is about obligation. I know that in the U.S., there are also indicative steps for that. I hope it will come to success also.

It will generate a very good starting position between the U.S. and the EU to come to the next level when we know what is our legal base, what we can do, we understand what you can do here or maybe third parties somewhere else in the world.

MS. PARNES: I think several of our commissioners mentioned that we are very hopeful that the U.S. Safe Web Act will be enacted into law, and that would really put us in a position to be able to share information and work much more collaboratively with our counterparts in Europe and elsewhere in the world.

I think, again, when we started our international program, I think it seemed very daunting to us that our legal frameworks were so different.

But we really quickly got over that. I look at an area now like privacy and I think that the European perspective on privacy and the U.S. perspective on privacy really are different.

But I have talked to colleagues in the Article 29 Commission, the working group, and our bottom line is the same. We all want to protect our consumers from injury. And I think that really gives us a leg up, because we have the same goals.

So it enables us to find a way to work together. We are optimists.

MS. HARRINGTON-MCBRIDE: It is a glass half full kind of Tech-ade.

Are there any questions from the audience? I feel guilty about having deprived you all of the opportunity in every preceding session. So I really want to know. Tell us now.

Okay. Well, hopefully many of you will be at our government-only day tomorrow and we will have an opportunity to further our discussion.

I very much appreciate you taking the time, both of you, to talk with us. I know Lydia, you have some concluding remarks you would like to make.

MS. PARNES: Yes. Thank you, Katie.

Just very quickly. First of all, to thank everybody who has been here. It has been really remarkable. I have to note that a lot of our panelists referred to movies over the past three days. My favorites are Woody Allen's Sleeper and

2001 Space Odyssey and, of course, Minority Report, which should be like the Tech-ade theme movie.

Movies really give us vivid images and they endure. But one that has come to mind for me is a movie that I actually watched this past weekend and it seems so particularly appropriate after the election, The Candidate with Robert Redford.

Those of you who have seen this movie will remember that Robert Redford is running for the Senate in California and he is not going to win, you know it, that's the deal. It's an election that he is not going to win. And there is a big upset and he wins. And the guy has no platform and he turns to his seasoned campaign manager and says "now what?"

And that's kind of a little bit like what I feel like. We have had the most unbelievable three days. And the question that we have, "okay, now what?"

Well, what we are going to do back at the ranch, back at the FTC is really take a very careful look at the amazing wealth of information that all of our participants have presented. We have really heard about visions of future technology, artificial intelligence, virtual world, social networking, RFID, and my favorite, the oven that you operated with a

cell phone.

We have heard the vision of the implications of some of these new technologies. And what particularly comes to mind is the very chilling PSA that Commissioner Harbour showed during her presentation, some of the real risks associated with social networking. And we have seen some really just charming presentations and Bongo, the stuffed monkey, and his battle to get on to a weather report online.

But I think that most importantly what we have learned from the insights, experience and vision from all of the people who have participated in this is that we all think about new things and think about some old things in new ways.

The world is changing. Consumers are changing. And the people who have participated, all of you have really helped us understand the role of technology in this transformation.

I want to first extend my thanks to everyone who has participated and all the people at the FTC, Katie, and the whole Tech-ade team who has done such an amazing job of putting this together.

(Applause.)

And tomorrow, it is not over. It is not over tomorrow. Law enforcers from throughout the United

States and around the globe will be meeting back at the FTC to discuss specifically what we can do together in response to what we have heard today. And the discussions are likely to have great bearing on how we approach law enforcement and policy development and advocacy and consumer education.

In short, I know that what we have heard today will be instrumental in evaluating how we perform the critical functions in fulfilling our core mission of consumer protection.

As Chairman Majoras noted in her opening remarks, the global hearings in 1995 helped to set the agency's consumer protection agenda for the next decade. Our discussions will provide a similar solid foundation for our next Tech-ade of consumer protection policy.

We will be drilling down into all of the data we have, and in the very near future we will be issuing a report presenting what was said during these hearings and discussing its implications for consumer protection.

So stay tuned and thank you all very much.

(Applause.)

MS. PARNES: We have one last video.

MS. HARRINGTON-MCBRIDE: We do. Our mantra

has been that the past is prelude. There seemed no more fitting end to turn to the reflections of a cyber patriot as we close.

(Whereupon, the video was played.)

MS. HARRINGTON-MCBRIDE: Thank you all very much.

(Whereupon, at 5:30 p.m., the hearing was concluded.)

C E R T I F I C A T I O N O F R E P O R T E R

DOCKET/FILE NUMBER: P064101

CASE TITLE: PROTECTING CONSUMERS IN THE NEXT TECH-ADE

HEARING DATE: NOVEMBER 8, 2006

I HEREBY CERTIFY that the transcript contained herein is a full and accurate transcript of the notes taken by me at the hearing on the above cause before the FEDERAL TRADE COMMISSION to the best of my knowledge and belief.

DATED: NOVEMBER 21, 2006

_____

BRENDA SMONSKEY