UNITED STATES FEDERAL TRADE COMMISSION
Washington, D.C.

RADIO FREQUENCY IDENTIFICATION:
Applications and Implications for Consumers
An FTC Workshop

June 21, 2004
8:30 a.m. to 5:30 p.m.

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

Reported by: Karen Guy and Susanne Bergling, RMR
For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
CONTENTS

Opening Remarks

J. Howard Beales, III....................... 5

Panel 1: The ABCs of RFID

Julie Brof, Moderator....................... 9

Panel 2: Current and Anticipated Uses for RF Technology

Lyle Ginsburg, Co-moderator

Charles Harwood, Co-moderator.............. 42

Remarks

Commissioner Mozelle W. Thompson........ 123

Panel 3: Implications of RFID Use for Consumers

Ellen Finn, Co-moderator

Frederick C. Livingston, Co-moderator.... 129

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
Panel 4: Looking Ahead: Competing Visions of the Future of RFID

Julie Brof, Moderator

Panel 5: Meeting the Challenge: Best Practices and Principles:

Elliot Maxwell, Co-moderator

Tracy Thorleifson, Co-moderator

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
MS. BROF: Hello. I'm Julie Brof with the Federal Trade Commission's Northwest Regional Office. I've spoken to a number of you, and welcome to the FTC.

Before we start today's proceedings, I have some important logistical and safety information to share with you. We're very low-tech here, so if you leave the building at any time, you'll be rescreened through security to re-enter, so make sure you bring some form of identification with you when you leave the building, and keep your IDs or your name tags on when you're in the building.

Please turn off all cell phones or pagers or set them to vibrate during the workshop, and fire exits are through the main doors at the front of the building or on New Jersey Avenue and through the pantry area, which is right behind here through a corridor to G Street, and in the event of an emergency or drill, please proceed to the Union Labor Life Building directly across Massachusetts Avenue, but don't follow me, I'm not sure -- oh, that way (indicating).

The bathrooms, very important, are located across the lobby, and there are signs right outside the conference area to direct you. Also very important, if
you would like to get some coffee during one of the breaks, we have the Sunspot Cafe in the building and Cafe Phillips right on F Street across the street, and there is information in your packets on where to go for lunch around here as well.

So, thank you all for coming, and without further adieu, I would like to introduce Howard Beales, the Director of the Federal Trade Commission's Bureau of Consumer Protection, our fearless leader and the reason we're all here today.

OPENING REMARKS

MR. BEALES: Thank you. Thank you, Julie. I would like to welcome you all to our workshop on radio frequency identification technology.

RFID has been described as the next big thing, but it's definitely not a new concept. It was originally developed during World War II and used as friend or foe technology. Fifty years later, the technology is still evolving, and RFID is still asking the fundamental question, "Who goes there?"

Another important question is, why are we here today? Why is the FTC interested in RFID? Well, today RFID is not just a business issue, but it's become an important consumer issue as well. It promises to reform, if not revolutionize, many corners of the
marketplace.

In the supply chain, it's transforming the track-and-trace process. At the same time, it's making transportation, health care and the food supply more efficient and safer.

We've got a great day planned. We're going to learn about the range of RFID applications from both developers and users in both the private and public sectors. We'll also be hearing from folks who are looking at the impact of these applications on consumers' lives, the benefits, like efficiency, product safety and access to information, and the potential drawbacks that may compromise the privacy and security of consumer data.

We'll be hearing from some experts with views on what the future will bring, and then we'll close the day with some suggestions on how to address concerns about RFID use.

This workshop is the latest in a series that was designed to help us educate ourselves and the public on emerging consumer protection issues. I want to thank our panelists who have traveled from near and far to help us do that.

I'd also like to thank those of you in the audience and ask that you participate. Your questions

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
and comments can help inform the discussion.

I also want to thank VeriSign, RSA Labs and
Texas Instruments for providing examples of RFID
technology and applications in action. During the
breaks, please take a look at these exhibits that are
out here at gallery which we are referring to as the
"Petting Zoo." We have great names for our IT projects
here. We have a refrigerator to hold spam, we have a
jet plane that matches numbers telemarketers called with
the Do-Not-Call List, and now we have a petting zoo.

I'd also like to say how pleased I am to see how
many industry members who are here today who are taking
the initiative to address consumer privacy concerns and
incorporate these considerations into the design and
deployment of RFID.

Consumer privacy is a critical issue for the FTC
and across the Federal Government, which is also well
represented here today, and for the business community.
The efforts to address consumer privacy take a variety
of forms, and that's as it should be.

The wide range of uses for RFID makes a
one-size-fits-all solution unlikely, but the common
objective should be transparency. There could not be a
clearer need for transparency than when a new technology
is deployed in new and different ways.

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
We need to tell consumers what's going on and why it makes sense, and we need to tell them in a way that doesn't place on consumers the totally unreasonable burden of comparing the privacy policies of the 40,000-plus items that inhabit a typical supermarket.

If we aren't transparent, fears may defeat the benefits that RFID may bring to business, government and consumers alike. We must not let that happen. Consumers need to know about this technology, both what it does and what it does not do.

Technology developers and users should consider what information is collected from consumers and why. Just because data can be collected doesn't mean it should be. And once that information is collected, it must be secured.

The FTC has certainly spent a lot of time over the past few years addressing information security issues, which are vital to good business practices. These considerations are not unique to RFID, but this kind of analysis is critical to re-assuring consumers about their privacy any time a new use of technology is contemplated. It's a challenge that is shared by the private sector and the Government.

I'm wearing two hats today. As the head of the FTC's Bureau of Consumer Protection, I'm looking forward

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
to learning about RFID, but I'm also interested in what's in store for me as a consumer, and we hope today's workshop will provide a basis for everyone to continue their efforts to advance this technology in a responsible manner and inspire more.

Before I turn it over to Julie for the first panel, let me take a moment to thank her for her hard work in organizing this workshop. Julie, along with Tracy Thorleifson and Chuck Harwood, all of our Northwest Regional Office in Seattle, have put together a great program. Again, we're very glad to see you here, and take it away, Julie.

PANEL 1

MS. BROF: Thank you. Hello again. With the help of our distinguished presenters to my left, this panel will explain, as the title states, the ABCs of RFID. Some of the questions we'll address are really the basics. How does radio frequency identification technology work? What kinds of systems are properly defined as RFID, and what are its parameters? And how does RFID differ from other technologies that serve related or similar functions?

Before we launch into the discussion, I'd like to introduce the experts sitting beside me who will be the ones actually answering these questions. First
we'll hear from Sue Hutchinson, who is a product manager with EPCglobal U.S. EPCglobal, as most of you know, is the joint venture of the Uniform Code Council and EAN international. EPCglobal's mission is to establish and support an internationally recognized standard for realtime automatic identification of any item in the supply chain of any company anywhere in the world.

As product manager for the EPCglobal U.S. Division, Ms. Hutchinson is responsible for the Solution Partner Program and for building subscriber services for the many hardware and software companies joining EPCglobal. Sue will give us an overview of RFID, including a video showing how consumers are interacting with electronic product codes. She will also discuss the applications of this technology, which will provide some critical context for the rest of today's discussions.

Next we'll hear from Dr. Daniel Engels, who is the Executive and Research Director of the Auto-ID Labs at the Massachusetts Institute of Technology. Dr. Engels was appointed to his current position in October 2003 when the Auto-ID Labs was founded in order to continue research related to the EPC system.

As a successor to the Auto-ID Center, the MIT Auto-ID Labs, under Dr. Engels' leadership, continues to
explore new applications of RFID technology. In his presentation, Dr. Engels will provide some important background on the evolution of RFID. He will also explain some facets of how it functions and how it differs from competing technologies.

Finally, we'll hear from Manuel Albers, the Regional Director of Business Development for Identification Products in the Americas at Philips Semiconductors. Philips Semiconductor is a global leader in the design and manufacture of chips used in RFID tags, and they have shipped more than 1 billion such chips to date. Philips' RFID-based technology is used across a diverse set of applications, such as supply chain management, transportation and security, all applications we'll hear more in-depth about today.

Manuel is a native of Hamburg, Germany, and has ten years of experience with smart card and RFID technology. Manuel's presentation will further explore how RFID is touching our lives already, which like Sue's presentation is a good preview of what will be addressed in greater detail as the day proceeds.

After we hear from our experts and discuss some follow-up questions I have, we'll have time for some questions from the audience, and this goes for the rest of today's panels as well. Each of you has some index...
cards in your packet. Throughout the panel, if you have a question, you can write it down, pass it to the closest end of your row, raise your hand like you're in school, and one of the FTC staff members will pick it up and give the card to me. So, if you need additional cards, you only have two right now, there are some where you checked in.

So, without further adieu, let's begin.

MS. HUTCHINSON: Good morning, ladies and gentlemen. I'm Sue Hutchinson from EPCglobal. We are a neutral, not-for-profit standards body that's working on technical standards for RFID and the information systems that support RFID. As part of my role at EPCglobal, I have the pleasure of working with a broad array of manufacturers, distribution partners, retailers, logistics people, hardware companies, software companies and integration partners throughout the world, all interested in driving towards a single set of technical standards for RFID and the information systems that support them.

So, you ask yourself, what is it about RFID that is so interesting to so many businesses around the globe that we're able to come together in such a cooperative fashion? I thought I would start this morning with a brief videotape to kind of give you a feel for what's...
exciting the supply chain about RFID.

(Videotape played for the workshop participants.)

MS. HUTCHINSON: Great. So, as the video pointed out, what we're here to talk about when we talk about RFID fundamentally is visibility and increasing the visibility within the supply chain around the globe. Now, with increased visibility, we look at two primary benefits. One is efficiency. If I can see where products are moving around the supply chain, I can be more efficient in the way that I move them, enhancing the ability for those products to make their way onto the shelf for consumers in a more rapid fashion.

More importantly, if I get better visibility in the supply chain, it helps me know where things are going and how fast it takes to get there. I can decrease the amount of safety stock or excess inventory that I hold "just in case" at various points in the supply chain. I can be a lot more efficient with the way that manufactured goods move from the manufacturer through distribution out to the final retailer and ultimately to the consumer.

The other thing that visibility gives me is assurance, not only assurance of where those products went, but they are, in fact, the products that I meant.
to send through the supply chain.

Let me finish this morning with a brief analogy, my tale of two pens. Now, pen number one I find out was manufactured here in the United States, and it went to a wholesaler, went into the distribution system of my local Staples, made it into the back room of Staples and then finally onto the shelf.

Pen number two was manufactured in Mexico. It was shipped to Canada where it was private-labeled by another manufacturer, made its way to that same distribution center and ultimately into the back room of my local Staples store.

Now, these are pens, so ultimately I don't care. I was just happy that they made it to Staples and I was able to pick up a box of them when I was running out.

If instead of pens we were talking about electronic components going into a computer system or a navigation system for an airliner or we were talking about prescription drugs or beef or even green onions, the ability to know the source of where those things came from, where they went and how they got to me as a consumer has a lot more importance than it did with just my two simple pens from Staples.

So, that's what we're going to hear during the course of the day from the rest of our panel of

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
technical experts and the rest of the panels today, is
to talk about simple supply chain visibility, how do we
become more efficient and more effective at moving goods
through the supply chain, through our global supply
chain, ultimately making them available to consumers in
a more expedient fashion, and how do we provide that
level of assurance, that chain of custody that lets us
know for certain that the goods we are about to
purchase, the goods we are about to use, are the goods
that were really meant for us.

Thank you.

DR. ENGELS: Thank you, Sue. Technology
problems always get us in the end. This is actually
perfect for the segue into talking about the technology.

One of the interesting things about RFID
technology is what Sue's just talked about, we're going
to be able to identify products uniquely, we are going
to be able to track and trace them throughout the entire
supply chains. That's a beautiful vision. That is
actually the vision of the Auto-ID Labs, vision of
EPCglobal. We're going to be able to improve our lives
by using RFID and by using the system behind that in a
secure and wonderful fashion.

Unfortunately, though, realities with the
technology, just as the realities with the technology
here, there's realities -- thank you very much -- there
are realities with the technology of RFID. For those of
you that have stood in line at a checkout counter and
watched bar codes get scanned and scanned and scanned
over and over again before the checkout person types in
the number, you understand that technology is foulable.
RFID is not the panacea. It is an enable technology
that has its limitations.

As has been stated before, RFID is not a new
technology. It has its roots dating back into all of
the wonderful electromagnetic radar radio
communications. The first large-scale deployments of
RFID technology were EAS systems back in the sixties,
the first large-scale technology of identification --
EAS has been called the one-bit, it's really half-bit,
identification technology. Either it's being read or
it's not.

The true RFID with unique identifiers first
really appeared commercially in the mid to late
seventies, and it's been used commercially ever since
then. You know, this is not a new technology. It's
been around for quite a long time, and in fact, if you
buy Ford automobiles, every time you use a Ford
automobile, you're using RFID. There's actually an RFID
tag embedded in that key of yours that's read when you
put it in the ignition, and that's actually part of your anti-theft system. You need that key, you need that RFID tag to be able to start the car. So, it's not a new technology. We should all be very, very familiar with it, but it's going to become more ubiquitous.

But I'm here to talk about the functionality of RFID and really to give you a feel for why is RFID not this panacea, not this wonderful technology where everywhere I go, I can read everything I want to.

Well, first, what is RFID technology all about? The functionality it has on it is a little bit of communication device. RFID tags communicate wirelessly. Just as your cell phone has an antenna, RFID tags have antennas. This is how they communicate with readers.

They typically have an identifier on them. This is radio frequency identification, after all. RFID tags will often have a mechanism for communicating with local tags in the field to be able to communicate with the same RFID reader at the same time. This is referred to as anti-collision algorithms. Some are better than others, and this is really a way that you can gain benefits of RFID by having multiple tags and being able to identify all of them, communicate with all of them.

Unlike bar codes, if you put lots of them in the field, you really need to simulate them before you can really
Now, advanced RFID technologies, more expensive technologies, can have on-tag memory. This is great for storing mission-critical information or caches of information. They have more functionality and they have algorithms on the chip itself, maybe on collecting data, maybe on-board sensors. It's really depending upon how much you want to spend, how much money you want to put into it, how much functionality you want to design into it.

At the high end of RFID, you'll get -- and like I say, this is really what a cell phone is. A cell phone has RF communication. You've got your antennas. It's got an identifier on it, in fact, a unique identifier -- most cell phones today have unique identifiers, and it's got additional functionality. You can actually do voice over the network, and it has a built infrastructure, et cetera. It's a perfect analogy. It really is an RFID device.

Now, because you've got this range of potential functionality, RFID devices are typically classified as passive, semi-passive or active. This is really referring to A, where do they get their power source, and B, how do they communicate.

Passive tags are the cheapest. They have no
on-tag power source, no battery, et cetera. They harvest energy from the reader's communication field. They typically do not have significant amounts of functionality. That is, on-board sensors typically are not part of the passive device, because it's only operating when the tag has power, that is, when it's in the reader field.

Semi-passive still communicate passively, so it is not actively sending out a communication signal like a cell phone, but they have an on-board power source that goes into one sensor, so they can keep a temperature history, run algorithms, has more functionality. This is very crucial when you're talking about the history of a device, particularly when it's out of communication range with a reader, very important in the cold chains, pharmaceuticals, et cetera.

Then, of course, active communication. Active is basically like a cell phone. You actively send out information. You can communicate with one another, and in the extreme, this may even be tag-to-tag communication. This is your ad hoc sensor networks type of functionality. Really this is the gamut of functionality. And RFID is a very, very broad swath of functionality, so from very, very inexpensive, low functionality, this is the identity tag being used by

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
Wal-Mart and being put on by the suppliers as well as many other retailers, this is what we're first developing as part of EPCglobal, and then we can move into the higher functionality, higher cost systems as we move forward.

Now, ultimately, the performance of an RFID system is determined by the regulations upon it. The more power you put out for communication, the longer your communication range, the more tags you can power, the more stuff you can go through to be able to communicate. There are three basic regions around the world, fairly similar in their regulatory within a region, but not necessarily the same exactly between regions.

When we talk about RFID, what are the main frequencies that are used? There is actually a range of frequencies. Each have advantages and disadvantages. We're probably all very familiar with 13.56 and 125K megahertz. These are low frequency LF and UHF actually. These are very short-range communication systems, low data rate systems. These are the access control systems used. These are what are used in the mobilization systems in your cars. So, it's not all new technology.

Now, we want long-range communication for supply chain, for example, we're going to use higher

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
frequencies, around 900 megahertz, for example. Again, great for long-range communication for passive systems but has limitations, of course. And there are other frequencies around the world where you may be able to use active communication, but power is such that you're not going to be use passive communications at those frequencies.

We're talking a lot about passive RFID systems, because that is the system that is going to be used in very, very short order in retailers and is being adopted by retailers around the world. When we talk about a passive system, there are basically three components. The tag, which is what you put on the object to be identified; the readers, which is what you use to communicate with those tags to gather information; typically the object identifier, so the reader knows where it is and the time it read it; and then you have the applications systems, which take that information and do something intelligent and useful with it.

Now, the tags themselves just have, you know, at the lowest cost, again, just have an RF interface, that's the communication, some sort of control for the communication, and maybe an application subsystem, that is, maybe an anti-collision algorithm. The readers have the interface communication control, application
subsystems, they maybe do some filtering, et cetera, and then network connection. That is, they can take that information that they've gathered and communicate it back to the application system, and then the application systems do something intelligent with it.

Passive systems, again, obtain their power or harvest all of their energy from the reader's communication signal. That is, if they are not close enough to the reader's communication signal, they're not going to be able to get enough power to power up to sync and to be able communicate with the tags. And again, power is regulated by local regulatory agencies. So, distance is really determined by what type of operating environment you're in.

We're talking a lot about "reader talks first" technology. That is, a tag is only communicating when it's told to do so by the reader. There are reader talk first systems or, I'm sorry, tag talk first systems, and that is when a tag enters a field, it will start communicating. If we're talking about extreme high densities of tags, those systems tend to be more inefficient, which is why reader talk first systems are being widely used and looked at as the deployment system of choice.

And of course, when we talk about an identity

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
tag, the tags being initially adopted, we're just
talking about tags that have an object identifier. So,
the data that they're communicating back is just tag
identity or object identity, very limited amount of
information on them.

And since UHF is the top of the discussion for
today primarily, because that's what's being widely
deployed, let's look at it a little bit closer. Some of
the advantages of using the 900 megahertz frequency
spectrum is it really is the best available frequency
range because of regulations for communication or
identification of objects greater than one meter away.

When you think about supply chains, back rooms,
warehouses, DCs, pretty much you're at least a meter
away wherever you are. It's very effective around
metals or can be made very effective around metals, but
again, requires good system design to work. If you put
the tags right next to the metal without designing the
system properly, you are not going to read it at all.
So, you have to use very good system design to make it
work around metals.

The range, again, is limited by power
regulations. In the U.S., you can get up to about ten
meters. One of the best systems on the market, best
case scenarios today, are ten meters. This is no
obstructions, wind blowing the right direction, no RF interference in any way, have very clean environment, ten meters is about the best you're going to get.

Practically, this means that you're going to get about three to five meters in a normal operating environment. You can get more, you can get less. It really depends on the tag design, the reader design and the interference of the system and the environment.

It's really good for non-line of sight communication. That is, you can read it through obstructions. You can read it through cardboard. You can read it through most objects, which makes it very, very good for identifying all the cases on a pallet, particularly as they're going through a back door or as they're coming down a conveyor belt.

It has a high identification rate, which makes it very good for reading tags in a high-density environment, moving through, again, cases on a pallet, where every case is tagged. And you can actually reasonably control the read zones. That is, if I want to read around a dock door, I can usually control the dock door environment.

Some of the major disadvantages of UHF communication is that it's absorbed by water. That is, if you want to communicate with tags that are located
around cola or water or other liquids, if you've got the
tag down near the liquid, you better be looking directly
at the tag; otherwise, you are not going to read through
that obstruction. That is, the water is going to absorb
the energy.

So, if you want to steal these tags, really what
you need to do is take them and put them in your armpit
and walk out the door. The reader is not going to be
able to read it, you know, a human is 90 percent water,
so it's a beautiful way to obstruct tags. That's by its
system design, if you rely upon the EAS systems just to
do that, though. No offense, Stan.

Now, while you can reasonably control the read
zones, it's also difficult to control. That is, if I'm
trying to read a passive tag going through a dock door,
while I can design the system to work around metal,
metal is also a beautiful reflector of this energy. I
can take this tag that I've got ten meters away, sitting
not even close to the dock door, and just because I've
got, you know, somebody's belt buckle -- they've got a
nice beautiful belt buckle, they walk by the reader
environment, I can get a beautiful bounce and I can read
this tag. It's a very unusual thing, that you can get
stray reads with UHF technology. So, I can control the
reading environment reasonably well. I also get some
spurious reads because of the nature of the technology, the nature of the communication.

Now, for the EPC identity tag, some of the key features of the identity tag features developed by EPCglobal and the Auto-ID Center, it's being adopted by corporations such as Wal-Mart, Albertson's, Target, where really the major retailers are driving its use within the supply chain.

The EPC identification tag has an EPC identifier only as its data content. That is, it's got an object identifier on it so I know what item I have, down to the inches level on an EPC, and purportedly for consumers, I've got a kill functionality. So, when I buy that tag, buy that object, I can have it killed electronically. I don't have to find the tag and rip it apart. I can just issue a kill command, and it will basically commit suicide. A little puff of smoke comes out -- I'm sorry, not the puff of smoke.

Now, for retailers, initially it's not going to be a worry, because these are not going into consumers' hands, but it is there, a feature that's been put in specifically to alert them, so that if you don't want these passive, promiscuous tags on your body, you just kill them, and that feature was designed directly into the EPC protocol specifically for that consideration.

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
So, a quick summary now that I've bored you with some nice technical detail. RFID technology really does have a long history. It's been in use for more than 30 years commercially in many applications. It has touched your life whether you realize it or not. The systems have great performance in some regions, not so great performance in others. It's really the regulatory requirements and limitations that determine the performance of these systems.

Passive tags, again, harvest energy from a reader communication signal. This is very important, because it means that it's really a not particularly reliable communication medium. Many obstructions, many variabilities in the environment can cause you not to be able to read a tag.

Again, the 900 megahertz passive tags being required for many retailers are in, best case scenario, less than ten meter read range, and they can be shielded by metals and by liquids.

Thank you.

MR. ALBERS: So, good morning. My name is Manuel Albers. I'm with Philips Semiconductor, and Philips is one of the leading manufacturers for those ID chips that Dr. Engels just referred to. I should probably show you one slide that we have.
Philips Semiconductors is a division of Royal Philips Electronics, one of the leading electronics companies in the world. I think it's about number three in the world, and is one of the top ten semiconductor manufacturers worldwide, and when it comes to identification technologies, we are one of the market leaders here with a track record of about 1 billion identification chips supplied into the market to date, so that's with respect to Dr. Engels' point of the technology is already out there around us, and I will now share with you where we already see this kind of identification technologies today and what kind of features make up these different types of identification technologies.

In general, when we talk about identification technologies, we are talking either about people who we connect through the means of identification technologies to services or we're talking about objects or goods that we identify and track through the means of identification technologies.

When we look at these two types or two classes of identification technologies, in the first place, for the people, we are talking typically about the type of smart cards. So, it's a feature that we are already pretty much familiar with here in Washington, D.C.,
where you use it for the public transportation, it's a smart card form factor, but it can also come in a smart token that you present to a smart com, for example, either for, you know, for the payment of your gas purchase or as a means of a loyalty system to collect points. So, these form factors are being used to identify people and to grant them access to services.

On the other hand, we talk about RFID, and RFID is all about identification and tracking of objects. These technologies have a purpose and have feature sets.

When we're talking about smart card technology, you typically then talk about a contact with a smart form factor or it can also be a token that can be easily inserted into a cell phone. You have -- what you find or what the goal is here is a combination of security and convenience, so that you have a secure means to access services, but at the same time, also make it convenient for you, so that you can, for example, even leave -- you can put the smart card in your purse or in your wallet, and you present it to a reader when entering the subway.

Typically, you find operating distance for these kind of contactless smart cards of about three to four inches or ten centimeters. What is important here is that when you identify people or when people access the
services is whether they're secure, and in order to make it secure, you're talking about different features and different functionalities.

So, for example, first of all, when you present the card to a reader, you want to make sure before the communication happens in between the reader and the card that both are allowed to talk to each other, so you have a neutral authentication. So, you really have to make sure, yes, I am allowed to talk to this reader, and the reader has access to this card, which means he needs keys for this.

What you are also going to encounter are encryption schemes. So, once both the card and the reader have authenticated themselves to each other, they talk in an encrypted way, so that somebody who stands next to it and wants to listen in, they can capture the communication, but they cannot understand it, because it's encrypted.

Another means for protection is a password, to also make sure that you as a cardholder are also the one who's authorized to get access to the data on the card. So, you will have, for example, on the one hand, you need to hold the card, and on the other hand, you need to pass it in order to access memory in the card when you present it to a reader.
And lastly, what you also see are those design features on the chip itself, so you make it very hard for people to try to break into that IC and to try to steal information out of the chip. So, you will have countermeasures on the chip level itself when you design and manufacture the chip that makes it very secure.

All of these features, however, also have a consequence. They typically drive the cost of such an IC. So, that's why you typically see the other costs of a smart card or of a smart token more in the range of more than a dollar and all the way up to $20-plus, depending on all the design features that you may include in the chip but also in the card itself.

Applications that we see out there, and I referred earlier to the point that we have already supplied some 1 billion RFID chips or contact identification chips, so where did they go? The bulk of them to date have gone into these kind of services for contactless smart cards to securely and conveniently grant people access to services. Public transportation is one of the main applications worldwide today. Just like in Washington, there are many other cities around the world who are already using this technology, primarily in Asia-Pacific and in Europe, but also increasingly now in the U.S., with not only Washington,
D.C., but also San Francisco, San Diego, Los Angeles, Boston, Atlanta and many other cities, including Las Vegas, are now going this way. So, this market today is worth about 500 million cards already.

Then you have payment applications, and you might have -- we have already seen announcements from both MasterCard, Visa and also AmEx to provide you with a contactless smart card that allows you to pay just by waving your smart card over a reader, for example, at a quick service restaurant, or in the future probably at the Starbucks, at the pump, and then that's where speed actually is important.

Another large area is access control, so a card -- you could be holding it in your wallet in order to access your office or something in the morning, and in a similar way, Dr. Engels also referred to cards for authorization. This market is probably also worth about 300 to 400 million transponders today to the various callup manufacturers and respectively to the car manufacturers that allow you to securely access your car, with not only the mechanical lock but also there's an electronic lock that requires a transponder when you slide in your car key.

Then the next step, you are going to get rid of your car key entirely. You will just merely contact the
smart card that you either carry in your purse or your pocket, and when you approach the car, it opens already the door for you, and because it realizes it is you, it also adjusts the seats for you, adjusts radio stations, and if you approach your car from the rear end, it opens the trunk for you, depending on how you have set the features.

And lastly, and this is probably the most ubiquitous application that we are going to see for contactless smart card technology, are our passports, so the U.S. Government personnel require and all other countries to deploy smart visas, also passports, that are able to hold your credentials, like your fingerprint or picture of the passport holder on a chip inside the passport, and when you come to the border entry, you present it also to a reader, just like your contactless smart card, and the officer is going to be able compare your face with the picture that is stored on the chip inside the passport. So, that is the people side of contactless identification technologies.

Now, when we look at the object side or the goods side, we really look at the RFID technology. It has a different focus. On the RFID technology side, we are typically talking about a smart label form factor, and to use one example on the picture that we see here,
it can also have various other shapes and form factors. Typically compared to the secure identification smart card technology, here you're talking about the functionality that Ms. Hutchinson earlier referred to as license plate information. So, really it's typically just a number that allows you to securely identify a specific good or product.

In addition to that, you can find additional memory residing in the chip that allows you to store more information about the product inside the chip. For example, before a manufacturer ships his product to a Wal-Mart, he wants to probably also make use of that RFID label going through his own supply chain, and for example, use that memory as a checklist when it runs through his own production, and at the end of the day, he will see that information again before he ships it out to Wal-Mart or to another retailer.

We find low to moderate security features, because these labels and these RFID tags are all about cost, and the less functionality you have on the chip, the cheaper you can make it, and thus also the cheaper the label is going to be.

So, the basic security features that you can find on these kind of chips are memory write protection, so that not everybody can just add information to that
chip, or a very basic encryption scheme. Also on these IC features is a destroy feature or kill switch, as has been referred to, that destroys all of the functionality of the smart label.

The reading distance is medium to long, so about 20 feet, and as Dr. Engels referred to, you can also get up to 30 feet, but this is really under optimum conditions. And again, it's typically for very low cost applications, and the price ranges right now are for RFID tags coming down from $2, all the way down to what is required today for the retail environment, closer to 5 cents or a couple of cents.

Applications that you see out there today range typically from supply chain management and the various kinds of supply chain management, being manufacturing automation, warehouse automation, processing services, baggage checking in airport, which is now becoming more and more popular and efficient, and on the other hand, you have asset management.

Most normally it's library automation, where you have self check-in and check-out terminals with books that you can take out of the library, but at the same time, you can also do automatic inventory control at libraries and identify books and those that have been misplaced just by hitting a switch or also by walking by

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
a shelf with books with a reader that allows you to identify the book that is placed in the wrong space.

If you have any questions, please also feel free to contact me by email. You will find my email address here in the slides, and I believe these slides are going to be posted on the Web, right?

MS. BROF: Yes.

MR. ALBERS: Okay, thanks very much.

MS. BROF: Thank you. We just have a couple of questions.

When you're talking about read/write capacity, does that relate to the memory function on a tag, and how does that work?

DR. ENGELS: With regards to the read/write capacity, that really is dependent upon how much memory is actually on the tag. When you write to silicon, you can, again, use the RF interface for it, and the read range is typically significantly reduced for the write functionality, because it requires more power to actually write to most memory technologies in use today.

Reading is simply trying to read out functionality or read out the memory contents, and when you think about how much memory is actually there, again, it's variable. Many technologies on the market today have sort of kilobytes or more of memory. The EPC
identity tag has just enough memory to store an object
identifier and an error detection code, typically on the
order of less than 128 bits of information.

MS. BROF: And when you talk about the
information that can be accessed from a tag and we're
talking about literally like a number or an
identification number, but the meaning of that
information only comes really when it's then linked to a
database with additional information, and how does -- if
the database is needed, what kinds of protections are in
place to limit access to it?

And if you're operating under a system where any
reader can read any tag, with then the next step being
getting meaning behind what information is on the tag,
how does that work or what kinds of protections exist?

MS. HUTCHINSON: We've been using the analogy
this morning of that simple identifier on the RFID tag
being like a license plate number. Well, if you have a
license plate number, you have to have a Department of
Motor Vehicles somewhere to provide the context for what
that number means, and this is literally the mechanism
that we use in the EPCglobal network. So, that small
identifier, that 96 bits of information that is held on
an EPC tag, is our key to a naming service that's called
the object naming service, works very much the way that
your internet browser works today with the domain naming
service, to translate a URL into a location somewhere on
the internet to be able to find the information, the
same thing is true with the object naming service. I
can go from that simple license plate number to a
location.

So, for example, if I have a product that came
from Procter & Gamble, as that tag is scanned, part of
the number that's on that tag may come up with the
number 0037000, which I can send to ONS, and it says,
oh, the information that you're looking for, you're
seeking, is in a server within the Procter & Gamble
network. So, we're talking about a server that is
behind the firewall at Procter & Gamble and very well
secured, because we're talking about some fundamentally
very sensitive business information.

By being part of the EPCglobal network, I get my
authorization and my digital certificate to be able to
then go as a retailer or another supplier or someone in
logistics, to be able to go to that network and ask for
more information about that number that I just read off
the tag. So, most importantly, the information is not
on the tag. It is secured behind the firewalls of
corporations, logistics providers and retailers all
around the globe.

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
MS. BROF: And now I have a couple of questions about the kill function, first just basically explaining how that works and who has the authority to kind of exercise that kill function or who I guess issues the command, then sort of two sides of the same coin, can it be re-activated, you know, kind of re-awakened, and then, would it be easy for someone to issue the command and destroy all the information, you know, or the ability to get information that would be useful, but maybe you shouldn't be able to do that.

DR. ENGELS: So, the kill functionality is a passport-protected command, so the reader can actually issue the kill command in normal command functionality mode, but a specific password is required of it as well. That password in the next generation will be 32 bits in length, and effectively that means it will take you several hours to guess the correct password to be able to kill a particular tag.

Dead does mean dead. Actually, I had a long conversation this morning about zombies and other ghostly features and characteristics of RFID tags, but no. Dead means dead forever and forever. Once a tag has been killed, if it is compliant with the EPC spec, it will never modulate back. So, it will never communicate ever again forever, never. So, the tag
information will never be modulated again by the tag; that is, it will never be able to communicate any information.

One functionality that has been talked about is that you can even erase the information as well if you have a like memory technology, is when you kill yourself, you kill the tag, you use the correct password, and then the tag erases all of its memory contents, so that even a forensic electron beam analysis of the tag will never receive what number was actually stored on it and that it committed suicide as well.

Now, who actually has the authority to issue kill commands? The answer is the owner of the tag. So, if you own the tag, you have the authority to kill the tag any way you want to, physically or electronically. If you do not own the tag, you definitely do not have the authority to kill anything. Just as it is with items today, you are not legally allowed to destroy items that you don't own. Even some that you do own, you're not legally allowed to destroy. So, those are the three tenets of the question.

MS. BROF: And I know we have our break in one second, but I just wanted to follow up, when you said the owner of the item, I guess, has that authority, I mean, would that be a system where consumers would have
pins that they would use to exercise it?

DR. ENGELS: If you as a consumer own a tag, you have the authority to kill that tag, and when you purchase it from somebody, you should either have them kill it for you if you want it as such or they should have transferred to you the correct password so that you can kill the tag yourself at some later date.

I believe most stated retailer plans with regards to kill functionality is that the retailers, when they sell an item that has a tag on it, will kill the tag at point of sale before it ever leaves the building.

MS. BROF: And the last question, changing topics, what's the status of the EPCglobal standard specification?

MS. HUTCHINSON: Sure, the Version 1 of all the specifications for the communication between the tag and reader as well as some common data elements and common communication techniques for those information systems that we talked about were modified by the EPCglobal Board of Governors last November, and there are currently more than 20 vendors worldwide that are already selling tags and readers to those specifications.

This is a technology in its infancy, though, and

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
as we deploy the technology, as we learn more in
implementation, we continue to revise those standards to
address what we're finding in our early implementations,
things like consumer concerns about privacy. So, we're
actively working on a second generation of all of those
standards, the first of which is due out later this
summer. We're probably looking at a second revision for
all of the standards related to the network before the
end of this calendar year.

MS. BROF: Well, thank you very much. That was
a good grounding, I think, for the rest of today, and we
have about ten minutes now before our second even longer
panel, so if you want to take a coffee break, we'll
reconvene at 9:45. Thank you very much.

(Applause.)

(A brief recess was taken.)

PANEL 2

MR. HARWOOD: Good morning. My name is Chuck
Harwood. I'm the director of the Federal Trade
Commission office in Seattle, and I'm pleased to be here
today to greet all of you.

This is our second panel of the day. It's on
current and anticipated uses for RF technology. For
this panel, after we finish this panel, you'll have a
sense of the breadth and scope of RF technology
applications or implementation, both currently and in
the near future.

We have a distinguished panel who will be
speaking with us today. I'm joined first of all by my
co-moderator, who is Lyle Ginsburg -- right, thank you,
trying to find my notes and talk at the same time, and I
don't read and talk well at the same time apparently --
and Lyle is the managing partner for Technology
Innovation in Accenture's Global Product Operations
Group. He was Accenture's board member at the Auto-ID
Center, now represents the company to EPCglobal. As I
said, he is the co-moderator, and he will be asking some
of the questions today.

In addition to Lyle, on the panel we have Britt
Wood. Britt is a Senior Vice President of Industry
Relations for the Retail Industry Leaders Association,
a/k/a RILA, R I L A. He's been with RILA since 1995,
and he also serves as RILA's main representative on
several external industry-related committees, including
the EPC Alliance for the last four years.

The third speaker or the second speaker,
actually, on the panel, is Simon Langford. Simon is the
Manager of RFID Strategy for Wal-Mart Stores, Inc.
Simon is responsible for the integration of EPC into
Wal-Mart systems.
The third panelist is Bill Allen. Bill is the Marketing Communications Manager for Texas Instruments (TI) RFID Systems. In this position, he's responsible for the marketing communication strategy and managing TI RFID's public relations advertising and trade show involvement.

The fourth speaker is Ken Fishkin, who's on the other side of the -- well, he's down there, okay. Ken Fishkin, he's a researcher at Intel Research in Seattle and an Affiliate Professor of Computer Science at the University of Washington. He has 15 years of experience in industrial R&D.

The fifth speaker is Paul Rudolf. Paul became Senior Adviser For Medical and Health Policy in the Office of Policy at the Food and Drug Administration in July 2003. He was a member of the FDA's Counterfeit Drug Task Force.

The sixth speaker is Lee Tien. Lee is a senior attorney with the Electronic Frontier Foundation in San Francisco, California, specializing in free speech and privacy.

And our final panelist member is Peter Sand. Peter serves as the Director of Privacy Technology in the Privacy Office of the U.S. Department of Homeland Security.

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
They will be speaking in the order I've introduced them. Before the panelists start, I will ask Lyle if he has a few thoughts he wants to share with us.

MR. GINSBURG: Thank you, Chuck.

Just a couple of context points before we get started. I have a feeling that we probably wouldn't be sitting here today talking about this if it wasn't for Wal-Mart. Now, I think that there are all sorts of great uses of RFID that have been out there for a while. I use many of them. I have my RF-based identification badge. I used to in my younger days run races, and you used to have these chips on your shoes that would record your start and finish times. I have a SpeedPass, so when I buy Mobil gas, I can pay for it that way, but I think the reason that we're here is because of some very recent events involving large-scale rollout deployment programs, and you know, Wal-Mart beget the DoD beget Tesco and so on.

So, I think that context is interesting and important, and if you look at where the technology is today, the current state, I think you got a pretty good sense from Dan Engels about where we are. You know, he talked about the fact that even 25 years later with bar code, you still have these issues of scan, rescan and rescan that take place, so you can imagine where RFID is
given its relative infancy, certainly in the way it's been talked about being deployed today.

So, you still get tags that get shipped to buyers that don't all work, or after they're applied don't work, or the performance isn't as fast as we want, the read rates aren't as high as we'd like, and we can't read all the things that we want to today.

The cost is still too high, you know, the lowest published cost that I've heard about for some of these tags, if you buy a million of them, is 19 cents apiece. If you talk to some of these companies about purchasing consortiums to drive the numbers up into the hundreds of millions, you start to be able to talk about things like 7, 8, 9 cents apiece, but still for many companies, that business case still doesn't work. We talk about even 5 cent tags for cases, pennies or less for individual items. So, we have a ways to go on the costs.

Dan talked about UHF frequencies and HF frequencies and how some frequencies work better at distances, some work better close up, and so we have to figure out if we want to start tagging individual items, which frequency are we going to use, so we can track something all the way through the supply chain.

If that's not enough, China threatens to invent its own system, and if that's not enough, you look up
RFID on your Google, and you get spy chips and so on.

So, what would any logical person conclude? Well, all systems go, of course. On with the show.

It's kind of funny, right, that those aren't the realities of today. Those aren't the relevant facts, yet we are moving forward. Why is that? Well, there's a pretty astounding panel that took place a couple of weeks ago at ECR Brussels where the CEOs of Wal-Mart, Metro, Unilever, Nestle, a few others, all talking about RFID, and I'm amazed that at that level they can spell RFID let alone have an in-depth conversation, which they did. They were all very knowledgeable on the subject, and their message was pretty loud and clear.

You know, we did invest in the bar code years ago. It was painful when we first got started, but we had to start to get to where we are today, and that was really the message of where we are with RFID. So, I think that sort of provides some context around why we are doing this given the realities of where we are. We're at the beginning of a marathon. We have a long, long way to go.

Here's an interesting quote for one of the CEOs where he said, "You know what? My CFO doesn't get this. Here we are focusing on the business value and the business case, and I've presented it to my CFO, and he
doesn't get it." But that's not important at this point, because it's going to be painful for a while until we get going and we start driving the benefits out, we get the scale, and we get a more robust set of technology in place.

So, this is a global phenomenon. It's not just happening here in the United States or even just in Europe. There are a lot of big programs going on in Europe, but we have active projects going on in Japan, Australia, Brazil. Any company, let's say, in the electronics industry that is part of any of these programs that our panelists are going to talk about are evolving, they have to engage Asia, because they have manufacturing and distribution operations in Asia, and so their Asian operations are going to have to get involved in this. It's not just a U.S. and European thing.

It's not just CPG. It's not just toothpaste and paper towels. It involves consumer electronics, electronic media, apparel, pharmaceuticals, and it's not just about case and pallet-level tagging in the supply chain. There are business cases and applications today -- and you'll hear about some of them here -- where it gets down to item-level tagging to really get the business value to solve the problem. That's a here

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
and now issue and phenomenon.

So, that's just a little bit of context. It's a marathon that we're in. You may look at any one of the individual piece parts and say, what's going on here? But that's not really the point, at least according to the CEOs of the companies that are actively involved in this.

Okay, Chuck.

MR. HARWOOD: Great, thank you. Thank you, Lyle.

Just a couple of comments before we start. For our panelists, be sure to speak into the microphone during your presentation. That's the only way are able to actually get the whole thing recorded and transcribed.

Second, if you have questions, I would encourage you to -- you'll find the question cards in your folders. You can go ahead and pull them out at any point during the presentation and hold them up or wave, and our trusty assistant in the back, Grant -- for those of you who want to turn around and look, he's waving now, or he was, you're too fast, Grant -- he can come around and pick them up.

Again, I'm going to ask each panelist, again, to limit their comments to about ten minutes, and Grant has

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
a sign that he will hold up to let us know that we are
going over the limit. It's supposed to say "Stop now,"
but instead it says, "Two minutes left," but that
doesn't mean you actually still have two minutes. It
means you should stop soon.

And finally, with regard to bios and things like
that, what I really did at the beginning was just the
first couple of lines of the bio of each individual. If
I read all of the bios, we would have been here for the
first 30 minutes. This is an incredibly impressive
group of panelists, and so feel free to take a look at
those bios, but we will begin with our first impressive
panelist right now. Go ahead.

MR. WOOD: I am Britt Wood obviously with RILA.

Thank you very much, Chuck.

Well, good morning, everyone. I hope you're
doing well this morning. Again, my name is Britt Wood.
I'm a senior vice president for industry relations for
the Retail Industry Leaders Association, pronounced
RILA. What I would like to talk to you about today has
several facets to it.

First, I'd like to tell you a little bit about
RILA so you can understand why I'm up here today
speaking to you. Secondly, I'd like to talk to you
about why our members are looking at RFID, why they're
interested in this and some of the benefits that they see related to RFID. I also want to give you a little bit of a reality check in terms of talking to you about where our entire industry is with regard to RFID. I also would like to share with you a little bit of the economics behind RFID that our retailers and manufacturers are looking at. I'll talk to you a little bit about some alternative uses of RFID that you may not be aware of that have been discussed within our membership. Finally, I'll briefly touch on what some other industries are doing and then take a real quick look at the future. So, let's go ahead and get started.

Who is the Retail Industry Leaders Association?

Well, RILA is an alliance of the most successful and innovative retailers and suppliers in the world today. Our members represent more than $1 trillion in sales annually and operate more than 100,000 stores, manufacturing facilities and distribution centers, both domestically and worldwide. We do have facilities in all 50 states as well as internationally, and our members employ millions of workers both domestically and worldwide.

Through RILA, retail leaders and the critical disciplines of the retail industry work together to improve their businesses and the industry as a whole.
Our mission as a trade association is to serve the successful and innovative retailers and suppliers through world class education, innovation and advocacy.

So, there is my promo. I hope I made it under 60 seconds.

Who our membership is I'm sure is a little more interesting than that. This is a sample of some of the retailers as well as manufacturers and service suppliers what we represent, AutoZone, Best Buy, Dollar General, Family Dollar, Food Lion, The Home Depot, Gap, Lowe's, Michael's Stores, PetCo, PetSmart, Target, Tractor Supply and Wal-Mart. On the manufacturing and service side, companies such as 3M, American Greetings, Coca-Cola, Eastman-Kodak, Energizer, Federal Express, Gillette, Hallmark, Johnson & Johnson, Procter & Gamble, UPS, Unilever, Time Retail, VF Corporation and Williams & Dickey.

So, why are folks so interested in RFID? Well, it's pretty simple actually. This slide best represents why our industry is taking such a close look at case and pallet tagging in the supply chain. The number I'd like to draw your attention to is the number in the middle, the 6 to 10 percent waste that is found through lack of visibility or poor visibility in the supply chain. This is an issue where we believe tagging at the case and
pallet level will give us the opportunity to enhance our visibility, and frankly, cut into this waste.

So, what are the benefits? I think you've heard some of our earlier panelists talk about the benefits. These are what we call success factors for retailers. Reduce on-hand inventory and basically reduce and have less use of safety stock. For those of you who aren't in retail, what safety stock is, on occasion, we're known to order lots of stuff because we're worried that we can't get more stuff in time when it sells out. In many instances, that stuff tends to not be sold and go to waste. So, that's obviously some inefficiency for us there.

Increase sales through reduced out-of-stock. Obviously if we have it on the shelf and we know where it is, we can increase our sales. Increase stock visibility and availability at the point of shipment, suffice it to say that means if we know where it is, it's going to be easier for us to ship it and transport it properly. This will lead to reduced transportation costs and reduction of shipping volumes, which will increase our efficiency. We'll also more accurately forecast, and stock replenishment will be another result of this, because we will have visibility in the supply chain and be better able to tell when and where things

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
are to enhance our forecasting.

Finally, we'll reduce shrink and theft in the supply chain, which is a large issue for our industry which we grapple with every day. If we know where product is and then we know when it disappears, it gives us the ability to sleuth that problem.

Potential benefits for the consumer on case and pallet tagging in the supply chain, I don't know how many of you here shop, but when you go to shop, you hate the feeling, as I do, when you show up and you're looking for a particular product and it's not on the shelf. There's a little SKU there and it says it's going to be there, but it ends up not being there, obviously a large amount of frustration. When we have better tracking in our supply chain, that is going to result less often. This will improve product selection, will result from the fact of the reduction in safety stock and the reduction of numbers that we may actually have to keep out on the shelf, giving us the ability to enhance the product selection for the consumers.

Product freshness on perishable goods -- actually, it is -- we are noting it on perishable goods, but it also works for any good with an expiration date, the opportunity for us to enhance the amount of time that the product is available before that expiration

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
date is a huge benefit to consumers, as you will not buy
aspirin and then have it expire on you three months
later.

Finally, easier identification on recalls. At
the case and pallet level, if there's a recall issued
and we know where those cases and pallets are, that will
give us the ability to bring that product back and
increase the ability of the retailer to get to that
product prior to it reaching the actual customers. So,
those are the benefits, both for retailers and we
believe for consumers.

What I'd like to talk about now is to almost
give you a little bit of a reality check, and these are
the two words we use most frequently when we talk about
where RFID is in our industry. I think even Simon would
agree that Wal-Mart, probably being one of the more
advanced companies, is still very much in this mode of
discovery and exploration, learning something new every
day, but at the same time also realizing that this
system by no means is a sure thing at this point.

You have heard about Wal-Mart, you have heard
about Albertson's, you have heard about Target or Tesco
and Metro with issuing some of the mandates and also
looking to implement the technology within 2005 or 2006.
Several other retailers have pilots in the field and

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
have not issued mandates in terms of telling their
manufacturers they'd like to have the cases tagged by a
certain time.

The first group I mentioned to you that I listed
by name are what we would call the innovators. The
second group are who's conducting pilots, and those
pilots are generally being conducted at either the 900
megahertz level or the 13.56 megahertz level. The
second group that's just conducting pilots are what we
would call the early adopters, and as we know in the
curve of adoption of technology, those are the first
two, and then the big portion of the curve is next.

The big portion of the curve, the majority of
the retailers who we represent are basically six to
twelve months away from even putting a pilot in place.
They're developing a plan, they're getting a team
together, but they're not ready to put a pilot in place.
They're taking a wait and see. They're trying to gain
some advantage by not having to learn the lessons on
their own, and at the same point, they are still very
much behind some of these innovators and early adopters.

Some of them are also focused on issues like
data synchronization, which is not a prerequisite to
RFID; however, without doing it, you will not reap 98
percent of the benefits that RFID can bring to your
organization. Data synchronization is a whole other topic for a whole other day, but it is something that's taking an enormous amount of time from retailers and manufacturers alike and is a large hurdle to overcome before they get RFID in place.

Interestingly enough, there are some retailers who frankly right now have very little interest in adopting RFID at all, and so they're trying to figure out the benefits for themselves, and they're conducting their own studies. So, that remains to be seen, exactly how that turns out.

The economics behind RFID, well, it's still pretty expensive, as you heard, 19 cents you heard Lyle say earlier, possibly buying at a million chips. Generally the range we use is 20 to 40 cents for the tags, and anywhere between $500 and $1,000 for a reader that generally reads about six feet, three meters. So, obviously that's a significant cost if you're going to put that in all your distribution centers and all your front doors. So, just that cost alone is what you hear a lot talked a lot about in the press.

However, what I'd like to show you now is part of a distance learning program that RILA has put together which also illustrates for you the cost factors involved in RFID, and I think Simon can echo these. The

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
hardware, which you hear most frequently about, that
does have some significant numbers attached to it, is
only 3 percent of the cost. It's a small amount.

The other significant portions of the costs
include the people costs, what it takes to train the
people, to get them in place, to get them more adept to
work with this technology. And then finally, the
software cost is roughly three-quarters of the bill, and
that's not talked about frequently. So, if you can
imagine that those numbers that I was just throwing out
to you represent a very small portion of the cost, you
can understand that this is a hefty project to take on
if you're a retailer, and it gives you a little sense of
the reality behind the investment that's required to
make this work within an infrastructure.

Real quickly, I'd like to talk about some of the
talked about item-level tagging and the economic
feasibility behind that. In fact, to take it to the
extreme, there's a particular member of ours who while
we were in a meeting was talking about the fact that
they sell items that are less than 5 cents. So, why
would you put a 5 cent tag on an item less than 5 cents?
Now, obviously that's the extreme, but it even leads to
the fact that there's a leading technology firm that has
come out with a statement that they do not foresee items

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
under $10 being item-level tagged until the earliest
2017. So, you get a sense of the infancy, where we are.

Oh, he's giving me the two minutes left. I have
so much good stuff, though. I'm going to go just a
little bit longer, I promise, and Simon will make it up
on his end. We made a deal.

So, I just wanted to give you a real quick sense
of the costs and everything that goes into doing that.

Finally, I'd like to talk real quick about the
alternative uses. Two things that have been discussed,
these have not been tested nor have they been piloted,
so these are simply discussions. One of them is using
RFID on very high-cost items for warranty information,
to frankly simplify the process, and that has been
talked about as when you give the consumers the option
to do that.

The other is, interestingly enough, you hear a
lot about this downflowing supply chain and using RFID
there. We've had some retailers express interest in --
well, I would like to use RFID in my reverse supply
chain. In other words, once the customer returns the
product to me, I would then like to slap an RFID tag on
it and track it up through my reverse supply chain to
better understand the inefficiencies and waste that's
taking place there and tackle that.

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
For the future, what do we see as a trade organization? We see a lot of supply chain use. We see a lot happening in the case and pallet level. We see a little bit of testing going on in the item level. We do not see widespread item adoption, widespread item adoption or use for at least ten years, and I think with the sense of the economics involved with this, you get an understanding of why widespread item adoption really doesn't make sense. There's a lot to learn in the supply chain.

And then one final comment, the interesting thing about retail is that unlike politicians who have a vote that's coming up in September, our customers vote with their feet every day. When it comes to RFID, we want to keep them informed. It is in our best interests to keep them informed, because if we do anything that could possibly make our customers uncomfortable, we will lose their business, and hence, it will cost us very dearly. So, I just want to leave you with that, that the retail industry is very interested in this technology to enhance their efficiency and make the customer experience better, not worse.

Thank you very much.

MR. HARWOOD: Okay, next we have Simon Langford with Wal-Mart.
MR. LANGFORD: Good morning. Thank you for the opportunity to come here today and share with you how we're using RFID right now and how we see using RFID in the near term.

I think interestingly enough, if you think back to the video that Sue Hutchinson showed, there was one thing in there that really sums up the use of RFID in the supply chain, and that is total supply chain visibility, right from the manufacturer right through to the retail store and to the sales floor, to the shelf, and that really provides total flexibility either for the retailer, the distribution center within the retailer, third-party logistics or the manufacturer.

Total leverage of RFID and the benefits touch on a number of these. The full potential across the supply chain is enormous. There are both collaborative benefits and also within four wall benefits within each organization, and so in terms of collaborative benefits, we spoke a lot earlier this morning about improved shopper experience through better in-stock on the shelf, thus providing extra sales growth not only for the retailer but also for the supplier, but more importantly, offering that customer service.

So, when a customer comes into our stores on a Saturday evening to buy diapers, for example, they're...
there on the shelf for them. They don't have to wait or ask for those to be pulled out of the back room or visit a different retailer. It's that visibility that is taking stock out of the supply chain, so we get in that just-in-time supply of product to meet the customer needs.

Then within Wal-Mart and Sam's, then as I come to a little bit later, store efficiencies, efficiency in the distribution centers, and likewise in the supplier as well. So, we've got collaborative benefits and internal benefits that we all need to realize.

If we take a snapshot of the supply chain then end to end, currently we have information when we receive products, when we ship products, but that's fairly limited. So, for example, we can't see when a supplier who's in the manufacturing process if they've got an issue. We don't see when they ship a product to us.

And third-party distribution or LTL, less than trailer load deliveries, that's very cumbersome to receive at a distribution center, very poor visibility, not only at the DC level, but at stores and clubs. We have got limited visibility of where that stock is. So, for example, we know that there's ten cases of product in the store. We don't know where in the store that is.

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
Is it on the shelf or is it in the back room? Today, we only know there's ten cases.

With RFID then, we are able to see back of the supply chain, to see if there is a problem with demand or production from the manufacturer. So, do we need to acquire additional product to maintain availability for our customers? Do we need to hire extra people to receive that product when it hits our distribution centers? RFID in the future will track merchandise at the carriers' terminals, and it will streamline receiving and check-in processes both at store and distribution centers.

When we talk about that streamlining, we also talk about accuracy as well, because as we all know with bar codes, there's a human factor in there that always can occur. So, getting an accurate perpetual inventory or on-hand figure is crucial to replenishing stores.

And then in stores and clubs at peak times, we have outside storage. We don't know where that product is, and it takes a long time for an associate to find and to replenish the shelf, but right from the word go, RFID would provide that visibility of where those ten cases are, sales floor versus back room. So, if we are out of stock on a product on the shelf and we can see that there's ten cases of product in the back room, we

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
can dial up the associate to go retrieve that product
and to merchandise it, even before it gets to the point
of being off sale. That's enormous in itself.

Think about street dates as well, about having
readers out to the sales floor as we move from the back
room. If we have DVDs that are supposed to go on sale
tomorrow, an associate tries to take those out today,
the system can alert to prevent that happening.

The next two slides are really what a lot of
people are seeing already from the RFID Center, but it
really comes in with where we allow readers at this
point in time, and that is at the back door receiving
doors of our stores and clubs and then in the back room
as we move out to the sales floor. So, at case and
level tagging, we can reach a lot of benefits that some
perceive as item-level benefits just from tracking those
cases and the intelligence in the software.

And then DC visibility, as we receive it from
the manufacturer, we can track it through our
distribution centers and then outbound to the stores and
clubs.

What we've got now is a short video which we
shot really for our internal associates to really show
them our pilot that we launched recently in the Dallas
area, so we show end to end where our weak points are

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
that I've just described there, but it also talks about
the future benefits and the future functionality that we
will receive from RFID, so if we can roll that video.

Okay, as this video is coming up, you will learn
things about eliminating shipping labels that we
currently place, print and place, on cartons that ship
out to our stores and clubs, and that all comes at a
cost, a cost to the supply of goods, which ultimately
the customer pays for.

(Videotaped played for the workshop
participants.)

MR. LANGFORD: I think from that you get a good
sense of why we're looking at RFID driving the
efficiencies and the supply to our stores.

Just one note on case and pallet, we do have
cases of products that are pack size one, so a
customer -- they are actually a selling item, and in our
pilot, we have three such items, for example, HP
printers, that are shipped through our distribution
centers as cases, and in that pilot, what we've done is
taken the steps to educate both our customers and our
associates on this, and if we can pull the slide up, we
can see an example here of how we've been transparent on
that education.

We've gone out with tear-off leaflets on the

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
shelf wherever these products are, and I think in Sue's video, there were some pictures of some flags on the shelf to let the customers know that we have that product on there with an EPC tag, and you can see here an example of the leaflet on shelf, again, to let customers know why we're doing this and that the product has got an EPC tag on there, and they've got a choice. They've got a choice then when they purchase that product to remove that tag. We do not have any readers on the sales floor. Our last read point, as you saw there on the video, is as we exit the back room out onto the sales floor.

And just to finish up, our consistent focus going forward with our sellers and our suppliers is that visibility of in-stock, driving increased sales, serving our customers better, driving our currency, and we can get equipment along with RFID equipment, that use of equipment, how effectively are we using forklift trucks, so on and so forth, but also cold chain compliance, I think Dan touched on this area, that there will be in the future tags available to monitor temperature. So, again, we can ensure that products are fit for consumption that have maintained chill compliance through the supply chain, both driving for internal efficiencies.

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
This slide just really summarizes the benefits which a lot of people touched on already about customer in-stock, reduced inventory, theft prevention, lower shrink in the supply chain, more efficient production planning at the supplier, smart recalls and the dramatic effect that can have, improved inventory control, and then ultimately, less inventory counting at the DCs, faster receiving of shipping, as I touched on at the beginning, and overall improved quality inspection.

Thank you.

MR. HARWOOD: Thank you, Simon.

Next we have Bill Allen with TI.

MR. ALLEN: Good morning. It's a pleasure to be here in Washington talking about my favorite subject, which is radio frequency identification, and I'd like to start off with a little bit of history of TI and our presence in the market space.

Of course, TI, we claim to have a strong heritage of innovation, perhaps the strongest. Mr. Jack Kilby, one of our lower-level engineers, some 30 years ago invented something that changed the course of history, changed the course of the electronics age and ushered in the electronics age, and in the year 2000 was awarded a Nobel Prize for his efforts, and of course, that was the invention of the integrated circuit.
TI has been in this RFID space for 15 years now, and we've surpassed the 300 million tag milestone just recently, and we are active participants in standards bodies around the world, ISO standards, IEC, ANSI, and of course, now EPCglobal. In addition, TI RFID has received a number of engineering excellence awards, marketing innovation awards.

Some of the milestones recently that we have surpassed, we've spoken about earlier, Dr. Engels talked about the immobilizer technology that's used in Ford products. In addition to that, if you drive a Jeep, Chrysler, Mitsubishi, Toyota, Lexus, any time you start your car, you're using RFID. You can't see it, but this is a transponder that's inside the head of the key. You're welcome to come out and look at the table, and we have got some examples here.

This is the reader that's inside the steering column. Now, they have a conversation, and they authenticate each other to make sure that the driver and the key is valid and you can drive away your car.

From there, actually the first application that TI RFID was involved in was livestock tracking, and that was driven by a problem, if you'll recall, some 15 years ago or so, actually in western Europe, there was an issue around mad cow disease, and identifying where that
livestock was that had the disease was the important thing, and being able to do that quickly and identify them very quickly and accurately would enable them to have less losses.

As you recall, millions upon millions of livestock were slaughtered because they could not track and trace where these livestock had been and what feed lots they were at, et cetera, et cetera. So, it's a wonderful implementation.

And of course, on December 23rd of this year, my phone rang when our PR agency called and said, Bill, there's a number of publications that would like to talk to you about livestock tracking here in the U.S., and of course, now it's on the radar screen of a number of associations, including the USDA, for identifying livestock. We had our first mad cow episode, if you'll recall, December 23rd. I remember it well, because I was on vacation.

Another application that was talked about a little bit this morning was library books. 3M has developed a wonderful implementation of RFID, and until most recently, you will, in fact, be reading -- if you keep up with RFID news, perhaps in the next week, there will be a press release announcing the Vatican has decided to use RFID to track books in their libraries.

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
and eventually some of the artifacts that are contained within the Vatican museum. It's a wonderful implementation of RFID.

And hopefully we have some ExxonMobil SpeedPass users out there -- thank you, Lyle -- hopefully you have this on your key ring. If not, go buy one -- or actually, it's free. You can just sign up for one. And 7 million customers in the U.S. are using ExxonMobil's SpeedPass to speed their way through the somewhat inconvenient activity of filling your car up with gas, and it's been also introduced in Japan, Singapore and a facility in other markets around the world. Shell has the implementation in Canada as well.

Marks & Spencer has been a long-time user of RFID. They are currently using RFID to track 4 million trays within their supply chain, and it's within their chilled foods and fresh foods supply chain. They picked up eight hours of store shelf life by speeding things through the supply chain more quickly. They also reduced their touch labor in managing these products, reduced it by 80 percent, and their estimation was that the ten-year cost of an RFID system that they implemented would be one-tenth of the original bar code solution that they implemented.

And here we are with a new innovation. Perhaps

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
you've seen this commercial. All drivers recognize
their cars. Some cars recognize their drivers. This is
Smart Access, a feature introduced in Lexus models last
year or this year, and it actually identifies the driver
as the driver walks up to the automobile and
automatically opens the door or actually unlocks the
door, sets the seat, as Dr. Engels said, perhaps adjusts
the radio station, makes you a cup of coffee, whatever
you want.

Here are some other implementations. Of course,
we're talking about warehouse and supply chain
logistics. This is Bloemenveiling, which is the largest
flower auction in Holland. Bloemenveiling has to manage
100,000 carts of flowers, about a half a million trays
of flowers, and get this, they process 37,000
transactions per day, and it's all done with radio
frequency identification, and they have cut their order
processing by several hours, they have increased their
accuracy of order fulfillment to 99 percent, which was
their ultimate goal.

Product authentication, when a consumer goes out
to buy something, if it's a high-value brand, it's a
good thing that that's an authentic item, and RFID can
certainly be used to authenticate high-value or branded
type items. But in addition to that, there's a

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
gentleman who plays professional football that I had the pleasure of spending some time with recently. Did you know that 60 percent of all sports memorabilia out there is non-authentic? So, Mr. Emmet Smith was very interested in using RFID to authenticate sports memorabilia and is going to become globally involved in this particular market.

Chip wafer manufacturing is another interesting implementation, and yes, we do indeed, as someone told me the other day, we do eat our own dog food. We actually use the RFID tags to identify wafer trays as they are processed, and it tracks what processes have been performed and writes the information to the tag.

Some additional implementations. Test tube tracking ensures the accuracy in tube identification, and also, this is to protect patients, after all. Major marathons was talked about, and my daughter ran the Portland Marathon here recently. I was able to track her progress through the race, for the whole time essentially.

Of course, livestock, protecting food supply and the quality of that food supply. Others, toll tags, I can't live without mine. Every day I use it on my way to work. It saves consumers time and also reduces emissions, because there are less cars sitting in line.
trying to get through the toll booth.

Event access and ticketing is another major implementation of RFID. If you go skiing in the Alps this year, chances are you will use an RFID-enabled ticket. Building access control, another very, very popular implementation of RFID.

There's more. RFID keeps minors safe in Great Britain. RFID keeps children safe at theme parks. RFID keeps hospital patients from getting the wrong blood type. It ensures that injured soldiers in Iraq get the right medical procedures. Here's a wristband that's used in this particular implementation. Tracking tree growth patterns in the State of Washington; tracking critical files in law offices; providing secure access for the Academy Awards; and in tracking salmon migration patterns, all kinds of many, many uses.

The state of the market? Well, RFID is not emerging anymore. There are more than a billion transponders deployed worldwide. RFID has been delivering an ROI for many, many businesses for many, many years. It's not something that's just come on the scene. RFID has created new markets. It's benefitted customers and consumers for many years.

When technologies come along, new technologies present new opportunities. It requires us to ask the
question, is there a better way to do something? It presents an opportunity to rethink, redeploy and re-engineer the entire enterprise. But for consumers, it provides new conveniences. It provides more safety and security.

So, let me get a few things straight finally. There is no perfect frequency. They're all good. They all have their own pluses and minuses, as was discussed earlier.

Another thing to remember, RFID is not a cure for bad business practices. If your supply chain is fouled up, throwing a new technology at it is probably just going to increase that.

The RFID industry has and will continue to respond to concerns about the technology, and to get this right, which we all have to do, it takes collaboration between technology companies, industry organizations, government agencies and end user and consumer groups.

Who wins in this scenario? RFID will bring new business opportunities and stimulate the high-tech sector, according to most pundits. RFID will help increase business profitability by having cost reductions and inefficiencies within the supply chain, and RFID, most importantly perhaps, will make the lives...
of consumers safer, more secure, easier and more convenient. So, everybody is a winner.

Thank you.

MR. HARWOOD: All right. Well, thank you very much, Bill, and next we have Ken Fishkin with Intel Research in Seattle.

MR. FISHKIN: Good morning, everybody. It's a pleasure to be here this morning. I'm going to be talking about RFID particularly in the health care industry, some of what people are doing now and then some of the more speculative, longer-range things that people are looking at in academia and research.

Health care is actually a pretty good monitor of RFID. First of all, as we just heard, a lot of the impetus for RFID or one of the big apps was the livestock industry, and it sort of has this unexpected benefit for health care, but for example, many RFID tags are very robust to heat and grime. Some of Bill's tags, for example, can survive sterilization and autoclaven, which is very nice in the hospital domain.

RFID can be worked with no special user action, you know, you're not doing this stuff. The fact that there are a lot more bits in the tag in the health care industry means that you cannot just say this is a bottle of medication X, but you can say, this is that patient's
bottle of medication X with this expiration date, and
they should take this many per day, they should not take
it with that, et cetera. You can pack all that
information in there.

And finally, because of the very high value
proposition in the supply chain as we've heard and we'll
hear more of later, cost is really just this huge
show-stopper, which may be true also here, because the
value proposition is so high. If you're going to keep
somebody from taking the wrong drugs, if you're going to
improve the health or stability of an elder, if you're
going to increase child safety, whether it costs you $40
or $50 worth of RFID tags is not going to be a
show-stopper.

Then there's another piece of technology that we
haven't heard much yet that is a nice match with health
care, which is a new wave of RFID readers. Most of the
applications -- actually, all of the applications you've
heard of so far use these dinner plate sized reader
antennas. In the petting zoo, they actually have some
of them out there that they're using, and the reason
that they use those is because they have this nice long
range, you know, couple of feet, couple of meters.

Well, if you're willing to give up on that range
and have an RFID reader with a range of like an inch,
then you can have these very, very small readers, and
there's a picture of one you see there about the size of
a quarter. I saw one last week about the size of a
dime. So, those things -- and that's so small that you
can actually sort of fit them into some nice niches into
some health care scenarios, which I'll talk more about
in a couple slides.

So, then when we talk about some of the
applications domains in specific, so within a hospital
domain, probably the most common thing that's being done
right now is this really goods tracking, really supply
chain management, except now what you're tracking is
where is this piece of equipment? Where is the crash
cart? Where is this patient's chart? Where is this
doctor right now? I just read about a project they're
doing in Dallas with tagging the babies, to make sure
that the right baby goes with the right mother and that
nobody takes the baby out of the hospital.

Now, that's really conceptually, though, really
similar to the supply chain issue, except now you're
just tracking a different set of things. So, I'm not
going to talk about that much more. I'll talk a little
bit, though, about these scenarios involving these
really small readers.

These small readers are small enough that you

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
can basically integrate them into high-value pieces of hospital equipment, and they serve really as smart connectors, to make sure that when you stick RFID tagged object A into receptacle -- RFID reader receptacle B, you did the right thing. People are talking about, as we just heard from Bill, with blood bags, to make sure you put the right blood into the right IV drips; with anesthesiology, gas dispensing, make sure you plugged in at the right time, et cetera.

There's another thing that we're actually about to hear about, an FDA movement to require RFID tags on pill bottles by 2007. So, one thing people have been looking at in research is let's pretend it's 2008, what can RFID do to help improve the quality of home health care and medicine? This is a field that's actually been entered by Accenture. This is a prototype that we get from Seattle where one of the things you can do is you can take these RFID readers, you combine them with a digital scale, so now when somebody takes the pills, you know not only that they took some pills, but how many they took, and you're looking at the weight difference when they put it back, and you can then integrate that into a system, whether in the home or in the hospital, that can do readings, reminders, prompts, it's time for you to take this, you didn't take enough of that and so
Now, a more speculative approach that we're pursuing is to say, okay, now if we've got a bunch of these objects getting tagged, if there are enough of those objects around you in either the hospital or home environment that are tagged, could we tell what you're doing by looking at what tagged objects you're interacting with at any particular time? This is something we call the invisible man approach. If any of you have ever seen invisible man movies, there are all these scenes where there's an invisible man, so you don't see him, but by what he's using, where he's using it and the sequence he uses it in, you and the audience all know what he's doing, that he's making a phone call, he's brushing his teeth, he's having a cup of coffee.

So, the idea is that if we can detect interactions with RFID-tagged objects, perhaps we can help in this activity assessment, and I'll talk more about how this could apply in two of these domains. First, in the elder care domain, all right, there's a case with elders with early stage kind of decline where, for example, any nursing home that takes Medicare funds has to fill out these so-called ADL forms. ADL stands for activities of daily living or things, as you see here, like using the phone, getting
dressed, making a meal, taking care of a kid, et cetera, and the caregivers have to fill out these forms, figure out, you know, did you get dressed today, what did you put on, how long did it take you. It's a very time-consuming, invasive and error-prone process.

Well, if the elder is willing -- if we can detect the elder's interactions with some of these things, and now because we're in research we get to take a look at things like this, the way we did this is we took one of these small RFID readers, and we integrated it with a glove, so as you pick things up, it knows it.

Well, obviously you couldn't ask an elder with early stage common decline to do that, but a few years out, this could be a bracelet.

Once you can do that, you can then at least give this information to the caregiver to help them track and assess how the elder's doing. This is actually one of the very few cases I've heard of so far where RFID can actually increase privacy in that it may not be all that great to wear one of these bracelets, but first of all, when you take it off, the data log stops, and secondly, it may be better than having a caregiver go into the bathroom with you or watch you get dressed, you know, at least now there's a pair of eyes that are nowhere in the room.

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
We're doing a similar project along this line in the hospital domain, more of the idea is to deal with med school student grading and training. They have these labs, these simulation labs, where these students go through these procedures, and again, the doctors need to take a lot of time and be in a lot of places to see what the students are doing in the simulation. This results in, for one thing, they're not doing the simulations very often, because they don't have the time for it, the doctor's time is vital, and secondly, again, they miss things.

So, here's a case where you can actually ask the med school students to wear gloves. So, they wear gloves that look like this. They go do their simulation, and they look at the data log and, again, use that to help infer and assess how they're doing the activities. This is a pilot project we're doing right now at the University of Washington in the Anesthesiology Department.

Since I'm here with a regulatory audience in Washington, I would also say that for our next step, we're trying to see if we can test this in the OR suite, still with no real people, but in the OR suite. And there are regulatory issues involving what RF frequencies can be used with what power in an OR suite.
and then be able to be refined. So, if any of you out there know what the answers are to those questions, please see me.

Okay, so now let's see a video. So, now Intel has made this lovely concept video showing some of the things we're talking about now, again, a few years out, where the form factor is a little bit nicer. The pad you saw before is now actually the thing on the lower right, this nice little stainless steel thing, and the glove has been replaced by a bracelet.

So, I am going to have to do that -- pardon?

Yes, escape you, escape you, double click you.

(Videotape played for the workshop participants.)

MR. FISHKIN: Hmm, hmm, hmm, I think I've bottomed out on everything. So, I think I'll just end the talk now.

MR. HARWOOD: Thank you, Ken, we appreciate the presentation, and let's see, our next presenter is Paul Rudolf, Paul Rudolf with the FDA. Dr. Rudolf?

DR. RUDOLF: Thank you very much. It's a pleasure to be here. I was a member of the FDA Counterfeit Drug Task Force last summer through the spring. The task force no longer exists. The FDA issued a report on counterfeit drugs, which you can all
find on our Web site, www.fda.gov, if you would like to
find more information about our approach to counterfeit
drugs and in particular about RFID.

I'm going to talk a little bit initially about
counterfeit drugs and then talk about how we think RFID
can be used to combat counterfeit drugs. Last summer,
there were a whole slew of reports of counterfeit drugs
in the distribution chain. It was the thought of the
Commission and the rest of us at that time that
counterfeiting drugs was a particularly heinous crime,
much more so than counterfeiting clothes or sporting
goods or anything else, and that we needed to be very
proactive in combating counterfeit drugs, preventing
them from being introduced into the distribution chain,
and we thought it was a potentially huge public safety
issue.

Last summer and hopefully now, we thought that
the U.S. drug supply was the safest in the world. There
was a very small number of counterfeit drugs on the
market. In other countries, it's a huge problem. Up to
50 percent of drugs in some countries are thought to be
counterfeit. Some classes of drugs, such as
anti-malarials, certain vaccines and others, are known
to be counterfeit, and there are regular reports of
people dying of illnesses that can easily be prevented

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
because the drugs are fake.
You hear a very little bit about the approach
that Nigeria is taking with counterfeit drugs. There's
a very active woman who's the head of their equivalent
of the FDA, and she's being very proactive, literally
closing down pharmacies who sell counterfeit drugs,
having bonfires burning counterfeit drugs.
Unfortunately, most other developing countries have not
been quite as aggressive.

We have noted at the FDA that there are at least
20 or 25 counterfeit drug investigations that are
opening every year, and that actually -- obviously, it
wasn't underscored, it minimizes the actual problem,
because each investigation usually involves hundreds of
people, hundreds of companies that are involved in these
schemes to introduce counterfeit drugs.

The counterfeiters in the world are becoming
increasingly sophisticated. They have access to a wide
range of very sophisticated technologies, so they can
very accurately reproduce the labeling, the packaging,
the bottles, the drugs, the pills themselves, with the
embossing, and it's really quite amazing to see some of
these pills that even experts can't distinguish from the
authentic products.

Now, of course, counterfeit drugs can be sold

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
over the internet, can be imported into the United States. So, we saw it as a huge potentially increasing problem, and this is just a graphic with the number of cases that we've opened.

So, with regard to the overall approach to counterfeiting, we saw that there were about five places in the drug distribution chain and the overall marketplace that could be addressed to secure the U.S. drug supply, and the first is the one that I talk about today, securing the product in packaging. Clearly the issue is about regulatory oversight, putting these people in jail, reporting, educating consumers, all that kind of stuff.

What we determined through our investigation, through gathering information, is that the most important thing to fight counterfeit drugs was the establishment of a reliable pedigree, and that's been talked about by some of the other speakers, the ability to track and also trace in reverse logistics exactly where a drug is going and where it's been, every single custodian of the product.

At the end of that, the pharmacist can actually look at a computer screen hopefully at some point and look at the entire history of the drug bottle that just arrived in his pharmacy and be very secure that that is
an authentic product. We determined or we thought that RFID could not only provide such a pedigree, but it's probably the best way of providing that pedigree, and it's the cornerstone of what we felt to be the fight against counterfeit drugs in the United States and in the world.

Now, in our report, we differentiated between mass serialization, which is the unique number or the EPC code which has been discussed and the actual mechanism for reading that and associating information with that number, which involves tags, readers and the information infrastructure that you've all seen. Obviously you've seen several tags, you've seen what the code would be.

Now, many of you are probably not very familiar with the way drug coding works now, but there's a code that every drug has called an NDC code, which shows who the manufacturer is, what kind of pill it is, is it Lipitor, is it Viagra, the number of pills in the bottle, a whole slew of information about the product. It's not clear what will happen, but if there is an EPC code associated with an individual bottle, it will probably include the NDC number as well as other information.

The reason why we differentiated mass
serialization and the infrastructure used to associate data with that code number is that two-dimensional bar codes can also contain a unique number and can also be scanned. We felt that RFID offered a large number of advantages to 2D bar coding for serializing pharmaceutical packages, cases, pallets; however, 2D bar coding can be used, and right now, there's a lot of discussion in the pharmaceutical industry about what's the best near-term way of serializing all packages of drugs.

Some drugs, as we talked about, as has been talked about before, are very inexpensive. People have talked about, well, why would you put a $5 or 5 cent chip on something that's only worth 5 cents? Well, there are generic drugs where a bottle of 100 might not sell for more than a dollar or two, and there are issues about whether RFID would be used on those bottles or what the business case would be for that, and that's one of the reasons why we have also thought that in some cases 2D bar coding could be used for certain products.

With the publication of our report, we established certain policies about RFID. The first was that it was our policy to encourage as rapid adoption as possible of RFID in the pharmaceutical supply chain, and based on the information that we had obtained and in

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
talking with folks at Wal-Mart, various manufacturers, being involved with the Accenture project, we felt that the widespread adoption of RFID in the pharmaceutical supply chain was reasonable or feasible in 2007.

What that meant to us was that we felt that not only could all cases and pallets be tagged with RFID tags, but a large number of pharmaceutical bottles, individual bottles, would also be tagged by 2007. That doesn't mean every single drug. We know that there are issues with certain types of drugs that would make it harder to put tags on them -- liquid products are a good example -- but we felt that the vast majority of drugs could be tagged in 2007, and quite frankly, in being out and speaking in various places and being in contact with folks, I don't think that we have any notion of pulling back from that right now. We think it's very feasible, and we think it's very likely to happen.

We've heard an awful lot about some of the drivers to RFID adoption. There are a couple within the pharmaceutical industry that I wanted to mention with a Florida pedigree law. There's a new law that was passed in Florida, and I guess most people don't realize it, but states regulate drug wholesalers, and drug wholesalers have been a major conduit for the introduction of counterfeit drugs, and the wholesalers
basically handle the product between the time they leave
the manufacturer and the time they arrive in the
pharmacy, and some products go through one wholesaler,
some products can go through 10 or 20 wholesalers
depending on the price of the drug and what the
marketplace looks like on that particular day and week.

Because of current business practices in the
wholesaler industry, it's not that hard to introduce
fake or diverted product back into the supply chain, so
Florida passed a very stringent law which requires
pedigrees on all drug products by July of 2006, which
means that every bottle of drugs has to have a piece of
paper attached to it that says exactly where that drug
has been from the time it was manufactured to the time
it arrived at a pharmacy.

Well, as we all know, paper is very hard to deal
with, and you can imagine every package of drugs in the
State of Florida having a sheath of papers associated
with it that people have to thumb through to figure out
where the drug has been is a pretty cumbersome process.
A lot of wholesalers have thought that they would be put
out of business, because they can't possibly manage all
that paper, especially big wholesalers.

I've been in some warehouses, McKesson and
Cardinal and AmeriSource, the three biggest drug

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
wholesalers in the United States, and they fill
thousands of orders every day, and they have millions of
drugs coming in every day, and there's just no way that
they could process all that paper. So, the wholesale
industry has sort of grabbed onto RFID as a way of
complying with the Florida pedigree law and being able
to handle all the shipments they get and all the
shipments that they start and initiate to get to all the
pharmacies in Florida, and it's quite likely that other
states are going to pass very stringent pedigree laws as
well, and that's going to be a big driver in the
pharmaceutical industry for RFID, because wholesalers
are going to absolutely require RFID to do their
business.

The one other thing that was mentioned
previously that is particularly important in the
pharmaceutical supply chain are recalls. It's
critically important to do recalls as quickly and
efficiently as possible, and right now, it's a very
cumbersome, paper-driven process, and a lot of consumers
don't know whether they have a bottle of drugs that need
to be recalled or not. With RFID, you can literally
only recall those particular bottles which are at issue,
and you can do it literally within a day. You can save
millions of dollars, save a lot of people from being

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
scared, and make sure that you recall the right bottles.

I'll skip this slide.

What we've done is we actually have made some regulatory changes to try and facilitate RFID and help focus the industry on using all the resources at its disposal to adopt RFID. The PDMA, the Prescription Drug Marketing Act, we made some changes with that to help the industry out. We're working very closely with sponsors and participants of pilot studies, notably with RILA and Accenture, to identify regulatory issues which could hinder the adoption of radio frequency technology. Because we regulate the manufacture of drugs and labeling of drugs, RFID poses a potential large number of issues there.

One of the things that we decided we would not do is we would not require RFID tags. We thought with the industry changing as rapidly as it is, technology advancing as rapidly as possible, that given the concern of the pharmaceutical industry with compliance, that we would probably stifle innovation if we required RFID, because everyone would just stop and figure out how they could comply with a regulation rather than continuing to innovate and make things better.

What we're doing right now is we're watching a whole slew of issues to make sure that they get dealt

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
with and that folks also can comply with our expectation in 2007. We're working on product quality issues. Does the electromagnetic energy affect certain drug products, where we know that some manufacturers are doing some studies right now to make sure that that is not the case. We've talked with industry about privacy issues. That's not something that we would directly regulate or be involved with, but we have the expectation that industry will deal with privacy issues, such as killing tags when consumers purchase drugs.

One other thing that we're interested in which I thought I would mention is the potential to use tags to provide information to patients. Now, this obviously is a two-edged sword. As was mentioned earlier, it's a huge potential conduit to give useful information to patients at the time they purchase drugs because of the product information that can be associated with the drug product. Obviously pharmacists would get that same information.

On the other hand, it's also potentially a way of advertising other drugs, advertising things which were not normally allowed to be advertised, and talking about off-label uses, because you can imagine that when you read a number, not only the good information about a drug comes up, but also, you know, manufacturers and

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
wholesalers can put ads in the database. They can put
other types of information in there, and so there's a
whole series of issues like that that we're concerned
about that we're going to have to think about as RFID
gets more widespread.

The last thing I want to mention are database
issues. Those were touched upon before, but in the
pharmaceutical industry, they're really extremely
important. Is the database that people are going to
have access to a distributed database where every
participant in the supply chain has limited access to a
small amount of information about the product, or is it
going to be a centralized database and everyone has
access to a lot more information? In the pharmaceutical
industry, that's yet to be worked out, and that may be
one thing that could delay the adoption of RFID.

Then the last thing that I want to mention
before I finish is that clearly RFID is not the end-all,
be-all. It's going to require people to actually use
it, and it's going to require some amount of due
diligence, and one of the things that clearly is going
to need to happen at some point is in the pharmaceutical
industry, if you purchase and sell drugs, you need to
only do business with people who are RFID-enabled and
use RFID.

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
A drug, even with RFID, a drug could clearly go to a wholesaler where there's no RFID, so it's not scanned in or scanned out, it's just in a huge hole for two or three days, who knows what might happen to that bottle, and then it gets shipped to another wholesaler who is RFID-enabled, and unless someone catches the fact that it took longer than it should have to get from this wholesaler to this one and think that maybe there is something going on in between, you know, you can't catch that.

Now, there are ways of knowing whether bottles have been tampered with. You can put the tags underneath the cap and put sealers around them, but people who are pretty smart can probably figure out a way to put fake pills in a bottle that has an RFID tag on it. So, one of the things that we're going to be looking at in the pharmaceutical supply chain is are all the participants only doing business with other people who use RFID.

With that, I will conclude.

MR. HARWOOD: All right, thank you, Dr. Rudolf. We appreciate your presentation.

Next we have Lee Tien who is with the Electronic Frontier Foundation.

MR. TIEN: Hi there. I'm going to sort of sound
the cautionary note about the privacy implications of
RFID, but it's not going to be a really privacy-oriented
discussion, because I think a lot of what we're going to
be talking about later this afternoon will focus on what
are the privacy issues. So, what I want to do today in
my time is talk about how government RFID use and
government-mandated RFID use is sort of a distinct
problem from the retail RFID privacy issue.

It's fairly obvious that government is moving
into RFID in a very big way. I have got a handout
outside that lists a lot of the current and contemplated
government uses. We can start with DoD's mandate in
October 2003 requiring all of its suppliers to use RFIDs
by January 2005. This is going to be a big potential
driver for item-level tagging.

The Homeland Security Department, from what we
can tell, is already using RFIDs in its U.S.-Canada
nexus, latest traveler card, and is talking about using
RFIDs in boarding passes. Obviously as people have
talked about, there are a lot of transportation sector
uses. This is an obvious one because of the economics
of transportation, the toll cards, the use of RFID
devices makes sense there from an economic standpoint.

Money, the European Union has been looking at
putting RFIDs into currency. We heard at one workshop

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
even within the last couple of months that there is actually a country in the world right now that has already embedded RFIDs into their currency, but I don't know which country that is. The Treasury Department is apparently looking at RFIDs in currency as an anti-counterfeiting device.

Schools, you know, this is something that we're hearing about a lot, that at a very low sort of grass roots level, people are looking at using RFIDs to essentially track students. There's a charter school in New York that's begun to record the time of day students arrive in the morning using RFID tags, and they want to use them to track library loans, disciplinary records, cafeteria purchases, visits to the nurse's office and so on.

So, what is special or different about government RFID or RFID-mandated uses? Well, one aspect of it is not special, but I think it's worth highlighting. Of course, it's the promiscuousness of the RFIDs in general. A lot of what we are concerned about in the privacy world does not manifest nearly as much if the RFIDs are not promiscuous; that is, there's security, cryptographic access controls and so on, but we're not expecting that to be seen in a lot of the kinds of applications we're looking at, such as in the

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
pharmaceutical area.

    The second is a certain degree of persistence; that is, we expect that RFID applications in the
government sector will not be intended or in the context
where we would necessarily kill them when we get the
device. The obvious example would be when RFIDs are
used or if RFIDs are used in, say, driver's licenses,
other kinds of ID documents, it's unlikely, given what
the Government would intend to use such devices for,
they would say, oh, yeah, go ahead and kill it.

    The third is their pervasiveness. If schools,
Post Offices, money, public transit, et cetera, et
cetera, are going to be all using RFIDs, then we should
expect to see a fairly interoperable and pervasive
network of RFID sensors, and that should be something
that we ought to be concerned about from the privacy
standpoint.

    Now, another government use example that EFF has
been very engaged in has been in the use of RFIDs for
tracking and tagging library books. We're based in San
Francisco, and the San Francisco Public Library, like
many other libraries across the country, are looking at
using RFIDs for item-level tagging of all borrowed
materials. Now, this has obvious advantages for the
library from a supply chain standpoint, but it has
concerns for privacy.

The obvious question of associating people's identity with the content or preferences that they have in terms of what they read, you know, is a traditional sort of reading privacy issue, and it has that persistence issue, which is that you wouldn't want people who were using this system for their tag to be killed when the first patron, you know, borrows the item. The whole point is that it's going to be coming back. So, how do you deal with that problem?

This is something that a number of the privacy groups have been trying to dialogue with the libraries about. I'm hoping, actually, in San Francisco to stop them from adopting RFIDs at all, because we've seen no indication that they have a clear understanding of the privacy issues or a commitment to using privacy safeguards there.

But I don't want to focus too much on the privacy aspects of that. There are two other issues that end up coming out of this from EFF's perspective. The first is a question of governance, and we're seeing essentially agencies as small as the local public library or a charter school to as large as the Defense Department with 43,000 suppliers and somewhere in the neighborhood of 45 million separate line items all

For The Record, Inc.  
Waldorf, Maryland  
(301) 870-8025
But where's the public governance as far as these kinds of adoptions go? Where is the public deliberative process in terms of fact-gathering, a privacy impact analysis or assessments, technology assessments? From a privacy standpoint, I do not want to see, you know, my state DMV or my child's public school being able to decide, well, we got a good deal from an RFID vendor, we are going to start tagging all the kids. I think there's a real need for a large-scale public deliberative process to govern government use of RFID.

The second point, of course, is that government use can't be separated from private sector use from a privacy policy perspective. We have to have a unified approach. And the first most obvious reason, of course, is that you have a spillover or subsidy effect from government use into the private sector.

Now, most privacy-endangering technologies like RFIDs can be analyzed in terms of market failure. Think about pollution. It might be individually rational for a company to pollute because the costs of pollution are distributed across society, but it is not necessarily socially or collectively rational for that individual firm to actually do so, because if everyone follows that...
same thing, you end up with lower air quality or water
group.

We think that in the privacy area, RFIDs
represent a form of privacy pollution, and we need to do
something to think about how we control the polluting
effects, and this is something that government would be
contributing to if government continues to adopt RFIDs.

Certainly whatever Wal-Mart does, the impact of the
Defense Department, of Postal Services, of schools, of
all of these government entities deciding that, yes, we
should be using RFIDs is going to, you know, radically
affect the demand for RFIDs and spread their deployment
much faster than otherwise would have been.

And then beyond just sort of these economic
effects, there is the legitimation effect; that is, if
your friendly neighborhood library is using RFIDs, how
bad can they be? If we have all of these sort of
supposedly beneficial or actually beneficial
applications of RFID, questions of when do we do
anything about the data privacy and tracking issues
associated with RFIDs will fade, will be left behind.

So, I have a few specific recommendations to go
along with this critique. The first is that we should
have specific legislative authorization with meaningful
privacy safeguards and not merely appropriations or

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
agency-level processes before governments use RFID. RFID should not be used by governments, at least not promiscuous ones, to eliminate anonymity, and that counsels against the use in driver's licenses, passports, ID cards and such.

You should not allow law enforcement, in general, to track people using RFIDs without meeting Constitutionally stringent privacy safeguards. And finally, we need to really consider whether or not public entities -- in fact, I would say public entities should not be allowed to gather information from private sector RFIDs and vice versa, again, without stringent Constitutional safeguards.

Thanks.

MR. HARWOOD: All right, thank you, Lee. Let's see, before our final speaker, Peter Sand, I wanted to remind you that if you have questions you would like us to ask the panelists, you can go ahead and fill out one of these cards that look like this, and they're in your packet, and if you wave them around, our faithful assistant in the back, Grant, will pick them up from you and bring them up front.

Okay, with that, Peter Sand, do you want to go ahead -- our final panelist here, then.

MR. SAND: Thank you, thank you very much.
My name is Peter Sand, and I am the Director of Privacy Technology within the Privacy Office of the Department of Homeland Security, which means I'm basically a human bridge between the people managing the technology and the people managing privacy issues, and I spend a lot of my time kind of shuttling information back and forth to make sure that the technology people understand the basic principles of privacy, and the privacy people understand the details of the technology that's implied.

I'm going to talk a little bit about the role of the Privacy Office within the Department of Homeland Security and then just go through a couple of quick examples to give you a flavor for the kind of work that we end up doing.

There are three basic measures that can be used to assess the value of any new technology. The first is, does it advance the organization's goal? The second is, does it make the experience of using that technology better for everybody involved? And finally, does that new technology sustain privacy protections?

At the Department of Homeland Security, we address that third measurement with the Privacy Office led by the Chief Privacy Officer for the Department, Nuala O'Connor Kelly. In fact, the mission of the
Privacy Office is to ensure that as the Department pursues its mission to secure the homeland, that it does so without invading privacy.

The Privacy Office is organized along lines of disciplines. There's an international focus. There's a disclosure focus, which is basically Freedom of Information Act responses, and there's a compliance focus and a technology focus.

Within the technology area, the Privacy Office seeks to operationalize privacy, which means to build privacy protections into the actual system development process so that privacy issues are raised and addressed as the technology matures, rather than leaving privacy as a final box on a long checklist of technology issues. This way, we can ensure that all privacy issues are addressed as the technology develops from beginning to end.

At the same time, the Privacy Office is an independent office serving advisory and oversight roles within the Department. The Chief Privacy Officer reports directly to the Secretary and also separately to Congress to report on how the Department's use of technology and operations affect privacy protections.

The key to understanding any need for information technology is the information itself. New
information drives everything. It drives the
technology, and it also drives the privacy assessment.
When information is personal information, meaning it
identifies a person individually, the Privacy Office
adds into the regular development process an additional
step of public notice.

The Privacy Office works with the folks that are
evaluating and building new technology to identify any
potential privacy impacts which may be raised by that
department, and we do that by asking a long list of
questions, things such as, what information is being
collected? Why is it being collected? Where does the
information come from? How will it be secured? How
will it be checked for accuracy? If there is an
inaccuracy, how do people go about correcting those?
Who will have access to the information? How will that
access be managed? And the questions go on and on and
on.

We work with the actual developers to build
answers to these questions so that as the technology
matures and is used more within the Department, those
issues are raised and developed at the same time, and
all that information is published directly to the
public. This fosters openness and transparency
regarding how the Government uses personal information,
and it ensures that when the Government, our Department, finds a new technology that advances the organization's goals and also improves the experience, that that use of technology also sustains privacy protections.

And this process is repeated over and over and over again. As a particular implementation of technology changes, as a system is upgraded or as new things are added to it, we repeat that process again so that the public is notified as things change about the implications of those changes.

I want to talk about two very quick examples. The first is tracking baggage through the airport system. These are things that the Department is looking at. These are not things that have been finalized or implemented. They're just avenues of pursuit within the Department.

In terms of tracking baggage, the purpose is to facilitate travel, to make sure that the bags go where they're supposed to go and actually get there and get there as quickly as possible. There are two issues that are raised. The first is an issue of scope. You want to make sure that when that job of tracking baggage is done, that the technology that tracks information related to that bag ends, that there's no continued broadcast of that information. The second issue is

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
education, so that as a process like that is rolled out, people understand what it is, how it works, what the implications are and what kind of access they have to the process itself.

The second quick example is border crossing. Again, the goal using the technology there is to facilitate travel. There's something like 330 million actual crossings of borders a year, and the goal is to get the appropriate level of information to the right people at the right time so that they can inform decisions in terms of facilitating that crossing.

The goal is to make that process work as quickly as possible, hopefully faster than the current process is now, and some of the issues that are raised are how much information actually needs to be transferred during that crossing. Can you use just a simple number that would trigger a record in a database that will present information to a screen rather than actually broadcasting the information that relates to that person directly?

And then another issue is control. Is there a way to use technology to give the individual person control over when information is broadcast, and is there a button that you could put on something that the person would say, okay, now that I'm here, I am going to send
you my information, and not have it be an automated, ongoing process?

That's a very, very quick review of what's happening in the Department of Homeland Security specifically with privacy. Thank you very much for your time, and I understand lunch is soon, so...

MR. HARWOOD: All right, well, thank you, Peter. All right, next we have got some questions, and Lyle, should we start with the cards or do you want to ask a few first?

MR. GINSBURG: As much as I relish the opportunity to torture my panelists here, I do travel in the same circles with some of these folks, so I think we'd rather get to your questions first, but I'll save some of mine for afterwards.

Paul -- and please make sure you speak into the mic, if you can -- how can we stop fake pedigree information being generated by counterfeiters?

MR. RUDOLF: Well, there's several ways to do that, and some of them are fully technical and maybe some other people on the panel would know better than I do, but aside from limiting access to database, if a counterfeiter had the money to actually -- had a foundry to produce fake tags, the tags all have an actual foundry number on them in addition to an EPC number.
So, there's one protection there.

If you know that Pfizer has purchased all their drugs from one manufacturer, you'll know that the tag might have a different foundry number on it, and you'd know that it wasn't really a drug purchased by Pfizer. Plus, each company will have a whole list of EPC numbers which are active, and so what a counterfeiter would have to do is they would have to hack into a database to know which numbers were active for which drugs, and then they also have to duplicate the pedigree information, because an unauthorized person wouldn't have access to the associated data.

So, you have the foundry number, you have the potential for the need to hack into the database to know which numbers are active, and then you have to duplicate the pedigree information, and even then what would happen is the bottle would show up in the system as a duplicate. So, theoretically, the worst thing that would happen is that both bottles with the same EPC number would be located hopefully very quickly and be tossed out of the system, because you might not know which one was counterfeit if the counterfeiter was able to produce the right pedigree.

So, you've got a whole slew of protections, and then you have a minimal effect on the end in terms of

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
when bottles are affected and thrown out.

MR. GINSBURG: Okay. Simon, why did Wal-Mart conduct an item-level tagging pilot -- question, Broken Arrow -- especially if it isn't currently using RFID at the item level?

MR. LANGFORD: As a lot of people know, we've conducted some field trial tests with the Auto-ID Center since about 2000. We started at the pallet level, case level and then started to look at item level, but it very soon came to light that pallet and case was the area to focus on, where the real benefits were in the short term, medium term, and so that pilot didn't go any further.

MR. WOOD: Real quick, and that really has been the findings. As I talked about, the economics behind item-level just doesn't make sense right now for retailers to implement. So, we think the tests have occurred, and there probably may be a few more retailers who test, but ultimately, the realization is that the real benefit exists in the supply chain, and that's really where significant dollars can be saved, and I think that's where you'll see implementation within the retail industry.

MR. GINSBURG: Okay. Lee, there was a claim that tagging library books with RFID is
privacy-invasive, but given that libraries already track who checks out what books, what does RFID add that is a privacy concern?

MR. TIEN: Well, the main one is if the RFID tags are not secure, i.e., they are promiscuous, then unlike a situation where only the library knows what the book is, anyone with a compatible scanner or reader would be able to get that information, and so the audience for the information is no longer simply internal to the library, but it could be anyone who can read it, and you know, this is a concern not only because of libraries themselves tagging but because the publishing industry is looking into the use of RFID tags for books generally.

So, you have sort of an issue of information and materials that are very regulatory of what people are thinking being capable of being associated covertly and at a distance with their identities.

MR. GINSBURG: Thank you. For Peter, border crossing, what would be tagged? Does this include passports with RFID tags, and if yes, where are we now with regards to RFID-enabled passports?

MR. SAND: My understanding is that it would just be an additional step in the identification cards that people currently use now. Right now, the actual
transaction is very manual, very kind of human-oriented, and the idea would be to take information that already exists and just facilitate that communication better. It's already taking place now. It's just a question of using technology to make it work a little faster, a little better.

MR. GINSBURG: Thank you. I'm going to throw out one of my zingers here. Britt, a fascinating pie chart with the costs, you know, as you said, everybody is so fixated on hardware costs, tag costs, reader costs and all that, yet you listed 3 percent of the cost of implementation as hardware, 73 percent software.

All right, simple math, using your sort of average of tag costs, 30 cents a tag, someone has 50 million cases a year that they send to Wal-Mart, that's a big number, and if that's 3 percent of the total costs, this thing is going to be enormous.

So, how do we rationalize the ratios?

MR. WOOD: You rationalize the ratios based on the fact that the percentage of software is based on the life of the project. In other words, there will be different iterations of chips, different iterations of numbers, and therefore, you are going to have to continually upgrade your software.

We have had discussions with different retailers

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
that have kind of talked about the fact that once we can
get the readers right and the chips to a basic level,
then it really is just kind of working with the software
and doing upgrades. So, in the lifetime of a project,
you will be looking at extensive costs in the software
side of the business. Up front, the costs really
resonate on the chip and hardware side.

MR. GINSBURG: Thank you, thank you.

Bill, one of the more sort of upstart, let's
call them pure play RFID companies that got a lot of
attention so far in relation to this CPG retail
phenomenon that's taking place now, more so than all the
other areas that you talked about, yet TI is still
beginning to write in a big way. What impact do you
think TI can have on this issue of cost? You're much
clearly bigger than any of those other smaller companies that
are in here.

I know Philips was up here earlier, and we
should ask the same question of Philips, but
representing one of the big guys, what do you think we
can expect to see in terms of TI's impact on that
market?

MR. ALLEN: Well, thanks. As a chip
manufacturer and one of the major chip manufacturers in
the world, we already make billions of things per year,
and we are also working on expanded wafer technology,
going to a larger wafer in order to get yield higher,and by doing a number of things like that, we feel likeand the math looks so far, it does look like we canreduce costs down to a level where we can achieve thatHoly Grail that's always been there of a 5 cent tag, andI think it's using economies of scale and, of course, asvolume ramps up, we can produce more, reduce prices, andI am confident that we can deliver that.

MR. GINSBURG: So, of course, I have to ask thefollow-up question. When?

MR. ALLEN: When? Well, as soon as you guysgive us lots and lots of POs.

MR. GINSBURG: Okay, fair enough, fair enough.

Okay, Paul, back to you. How do you plan tobalance the FDA's refusal to create regulations on RFID,per your final comment, and against your final commentthat the FDA will require manufacturers to only workwith wholesalers who use RFID?

MR. RUDOLF: Well, if I used the word "require,"I misspoke. The FDA can't require that people dobusiness with each other, so if I said that, Iapologize.

What we've been doing is working with industryto try and get industry to adopt internal good business
practices, and in fact, the Healthcare Distribution
Management Association has a set of business practices
that they have posted on their Web site for wholesalers.
A lot of manufacturers have adopted business practices
that limit sales to certain wholesalers that might use
certain criteria, and I think that's one of the things
that we'll at least discuss with various industry
participants, is how could that happen. We would not
require -- we can't require that.

And with regard to not requiring RFID, we
actually think the industry will adopt RFID more quickly
if we don't require it.

MR. GINSBURG: Okay, Chuck.

MR. HARWOOD: Yeah, let me ask a question of
Ken.

Ken, a lot of the applications -- to, say, get
the data, scan the items, Ken, a lot of the applications
you talked about seemed to involve the use of
tremendously small RFID chips. I wonder if you have a
sense of, you know, how close we are to actually having
the chips that are small enough to be usable in sort of
the applications you described, the home or hospital
applications.

MR. FISHKIN: Well, it depends on -- you mean
the tags or the readers?
MR. HARWOOD: Actually I meant the tags, but if you want to address both of them, that would be good. Actually, the readers, too, I meant the readers as well.

MR. FISHKIN: Well, okay. On the reader side, as I showed, there are readers out there, you know, today, pretty new on the market, but there are readers today that are really very small. Like I said, there's one from a company called Innovision which is basically the size of a dime. Now, you have to add things to that. You add the battery supply, you need to add the wireless communication, you need to add the antenna, et cetera, but still, the overall package, like I said, today can really be pretty darn small, you know, they're putting them in a Nokia cell phone. So, on that, I think, you know, we're pretty much there.

On the tag front, again, even though I'm from Intel, we're not making these chips, we're just buying them from people like Bill, and the tags they have today are kind of awkward. They're a bit big, but the vast majority of the real estate is actually antenna. The chip itself is really small. So, it really becomes a function of sort of what read range you want, how robust you want the reads to be, you know, so do you have to, you know, hit it just right.

So, for example, in the anesthesiology thing
which we're doing now, and there again, we literally wheeled an anesthesiology cart into our lab and started tagging the stuff that they use today, and it's a problem on some of the things, but not by much and not by many. The best ones we have are actually -- in fact, the best ones we have are ones from TI which are about the size of a quarter, and then there are some from Alien which are about the size of like a pinky finger, and so it would be nice if they were smaller, but those are good enough to get you most things.

The bigger issue we have is something that I touched on briefly earlier, which -- in fact, this is the exact type we use, thank you, so-called laundry tags. The bigger issue is, at least in this environment, we have a lot of stuff that's metal, and these things really don't like being near metal, and that's really a more severe problem, and that I think would require more work.

MR. HARWOOD: Thank you.

Peter, does DHS intend to provide technology companies liability protection with regards to privacy matters similar to the Safety Act which protects companies from legal liability for developing technologies to combat terrorism?

MR. SAND: I have not been part of any
discussion about liability protection from DHS. I think what's more likely is that there would be a long series of open forums of discussion, so that people can put out in public what they see the issues to be and then design from the best ideas that come out of those discussions, so that a lot of the issues are resolved ahead of time. That I think would be the most efficient way to resolve those kind of issues.

MR. GINSBURG: Maybe for Bill and Ken, is an interconnected public network of readers truly possible to read all RFID tags? How would you manage the terabytes of data?

MR. FISHKIN: Well, how long do we have? Let me get to the first part of that, and then actually people like Jim Waldo would actually be much better to answer the second part of that, and he's on a panel this afternoon, so maybe I'll defer some of that.

Interoperability is a problem. There are multiple frequencies which are mutually incompatible, but it's getting better. The number of frequencies is going down, particularly driven by people like Wal-Mart. Standards are emerging, the EPC standards, things like that. So, it's getting better.

There are readers, though, today that can read two or three of these, which gets you most of them. So,
I think from sort of a technical engineering point of view, it's doable, and it will become more doable within a few years.

As far as the data access, I think I will happily save that for maybe later in the day, unless, Bill, you want to address that.

MR. ALLEN: Well, on the multi-protocol reader side of things, when you put that requirement in, performance is degraded, because it has to frequency-hop and do a variety of different things. So, there's tradeoffs for anything that you do no matter what technology you're applying. If you want it to work harder, performance will be degraded.

And then on the data side, yes, that's a very daunting question, is what are we going to do with all this data? And of course, a friend of mine who works as an analyst in the retail sector did his own little calculation one night when I guess he couldn't sleep and wanted something to do to occupy his time, and so, Simon, he calculated about how much data Wal-Mart would generate in one day, and I don't remember all of the details of it, but it was something like if you guys read, you know, so many tags in so many stores, it would generally 7.6 million terabytes of data per day.

Obviously that's a fairly daunting number, but

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
again, there will be solutions that come along, because, you know, you can have a savant server that says, do I need this data? No. Okay, I ignore it. Do I need this data? No, I ignore it. Did something change? Yes, I need this data. Therefore, I'll write that data. So, there will be schemes that will be developed in order to reduce the amount of data that is generated by RFID.

MR. GINSBURG: Simon, any thoughts on how much data you're going to be --

MR. LANGFORD: I think the last comment there is the crucial one, is keeping the data or acting on the data that you need to, the fact that a tag may go past a reader 30 or 40 times in this room, but I don't care about that. What I care about is when it leaves the distribution center and arrives in the store. We keep all of the data now on movements of merchandise through our supply chain. At least the RFID is plugging some of those holes, or as I intimated earlier, knowing when a case moves out to the sales floor, where is it? Is it in the back room or the sales floor? So we can direct associates to go and find that product in the back room. So, it's just taking those extra read points and acting upon that to help our associates serve our customers better and more efficiently.

MR. GINSBURG: Well, while you've got the mike,
we've got a series of retail questions lined up here, some for you and maybe Britt can help you out here a little bit.

One specifically for you is does Wal-Mart have an estimate of when all Wal-Mart DCs and retail back rooms will have RFID readers?

MR. LANGFORD: We're currently working with our suppliers. We've recently announced last week our expansion through the next year, where we'll be in something like about a dozen distribution centers and up to 600 stores by the end of 2005, for January 2006. We're working with our suppliers on that expansion plan to get their feedback and expectations of theirs.

MR. GINSBURG: For you and Britt, if RFID tags permit larger numbers of items in stores with fewer stock-outs, will retailers reduce shelf facings and/or slotting allowances as adoption becomes more widespread?

MR. LANGFORD: We have no plans to do that. I think with this technology, as we've seen where other people have implemented it, there are lots of "wows" or "ah-ha's" that come out that really tell you things about your business that you don't understand, and we're starting to see that in some of the early data that we're seeing now of where maybe a business process falls down, you know, and why does product take so long to get

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
to the customer, to the shelf, but no, there's no plans
to do that.

MR. WOOD: And I echo that sentiment. The
majority of the members who we've talked to who are
looking at this, that's really not a point of
discussion. It really is about the efficiencies that
Simon talked about that they really feel is the thrust
of this technology right now.

MR. GINSBURG: And the last one, Simon, is
recognizing that this is a long journey, all right, we
have to get to scale and critical mass to really get a
lot of the big benefits, can you describe when the --
not so much the benefits, but the profitability side of
it, when you expect to start to see that and when you
think that will be on the horizon for the suppliers?
Clearly day one, it won't be there, right?

MR. LANGFORD: In terms of our suppliers, and I
wouldn't want to speak for our suppliers, and every
supplier is configured differently in supply chain
makeup and the volume of products that they service and
the number of out-of-stocks that they may have. So,
we're trying to focus on things that deliver return not
only for Wal-Mart but directly to our suppliers as well,
and the biggest thing is the in-stock position and
increased sales that I mentioned.

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
We would start to see that and start to change processes in our stores and distribution centers from January, to start to go down that path, and you're right, we will hit a critical mass when that starts to change.

And just to come back on one thing about the cost of implementation and the cost of software, et cetera, we've approached this in a very simple way, a little bit like the data I mentioned and how we are keeping that, which pieces to keep and which not, and we're taking the stance that if we start it at a point where we integrate the EPC and take that as though we're reading a bar code, just that serialized number, what kind of things can we do within the application to be more efficient, and then that's our starting point.

We are not whooshing off to change our legacy systems and all our applications. So, it's one byte at a time, and we haven't increased our IT spend over and above what we normally budget for year after year, and that will continue, and this will just be another initiative, similar to the bar code and other things we've implemented, whether that be -- and so on and so forth, that we will just have iterations through each year and continue to improve.

MR. HARWOOD: All right, well, I think that's

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
all the time we have for questions. I apologize if we
didn't get to all of them. We had a number of them that
were still in the pile here, but we simply didn't get to
them. I do apologize for that.

I would like to thank all the panelists, and I
hope you will join me in a round of applause for them.

(Applause.)

MR. HARWOOD: And next we have Commissioner
Thompson, who is with the Federal Trade Commission, and
maybe if the panelists would just stay up here, wait
here and we'll go ahead and facilitate things a little
bit, you will have an audience as well.

Commissioner Thompson has a few words for us
before our lunch break, and he's obviously a Federal
Trade Commissioner, has been at the FTC since --

COMMISSIONER THOMPSON: Forever.

MR. HARWOOD: -- forever, yes, well. It doesn't
seem like that long actually, but anyway.

REMARKS

COMMISSIONER THOMPSON: I hear the collective
growl of stomachs all through the room, so I should keep
it quick.

Well, good morning. Thank you all for being
here. I see a lot of familiar faces, and I'm happy to
see a range of people attending this conference, from
industry, government and public interest groups, and I appreciate you all being here to discuss this very important issue.

Two areas to begin with, one is that my general disclaimer, my words today are my own and not necessarily those of the other Commissioners, and the second is all of your tags have tracking devices. We'll know where you're eating, and if you're not back here on time, we will bar you from the room.

But today, we're here to talk about RFID, what it is, how it can be used, what it means to business and consumers alike. Now, I think our workshop today is an interesting one and an important one because it represents the first really broad-based conference on the subject, and it will give us all an opportunity to set aside some of the misconceptions we have about RFID and to discuss the problems it creates but also the potential benefits.

So, today is an important first step in a process that I hope all of you will view as a continuing dialogue, and I'm sure there will continue to be public debate, so an opportunity for continued communication, and importantly, cooperation on this subject begins right here.

Today, we learned that RF technology has
actually been around for quite some time. It's currently in use in a variety of contexts. I just drove back from New York last night with my E-ZPass, so there's lots of examples.

We've also had a chance to learn a little bit about the nuts and bolts, about how RF technology works, starting with how the chips and the readers communicate, and we've heard about what this technology can and cannot do and a little bit about what its likely economic impact will be.

Now, we also heard from experts who are basically putting RFID to work in manufacturing plants, in distribution centers, in the retail stores, medical facilities, and in light of the breadth of potential applications, it also should come as no surprise that it poses a variety of privacy, security and other types of questions.

So, having heard a little bit about the potential benefits and risks of RFID, I'm especially looking forward to this afternoon's discussion, which will address a little bit more concretely how this technology will affect consumers now and in their daily lives in the future.

For example, streamlined supply chain management can, of course, benefit consumers when they shop,
creating more efficiencies and hopefully potentially
lowering prices. I like that.

But RFID may also benefit consumers more
directly if merchants move toward an item-level tagging
system, where consumers could buy things more quickly
and return them more easily and perhaps, more
importantly, recover them if they're stolen.

It also has some potential to have improved food
and product safety, but they all have questions, too,
these applications. Will such a system result in more
tracking of consumers? Will it facilitate their
profiling? Will it expose consumers to unwanted or
annoying corporate marketing? Of course, we know that
never happens, right?

Just what kind of data, how much will be
generated in a world where RFID is ubiquitous, and where
will this data go? All of these questions raise the
issue of what industry's responsibility will be, and of
course, what should be the Government's role?

This afternoon's panel, or perhaps more
accurately debate, on what the future will bring will
discuss this complicated and fascinating question.

Though I'm not sure of what this afternoon's
discussion's outcome will be, I am confident it will
take longer than today to find the answer or what the
appropriate balance will be.

But today, we have an opportunity to have a good start, so I hope we hear some creative approaches to addressing the challenges that we all see before us, and as we close the workshop, we'll have a chance to talk at least at the outset on what kind of best practices and principles might be helpful here, and during that discussion, we will hear from companies who have considered consumer privacy issues and have attempted to accommodate them in their RFID trials, and that's not just here, but also abroad as well. We'll also hear some privacy experts who have seen similar challenges and focus on translating industry efforts for meaningful choices for consumers.

Now, I know that none of these approaches alone may work for all of the questions that we have on RFID, but together, they may hopefully lead us to meeting the challenges that will be laid out today. At the very least, they will help to inform the policy makers and businesses and consumers about how to better balance the risks and the benefits posed by RFID.

So, I hope to see you again talking about this subject, hopefully not as defendants but as participants in an ongoing dialogue to find what the appropriate balance is for RFID and to also talk to consumers about

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
how they can make meaningful choices in using new technology. So, thank you very much for coming, and I hope to see you after lunch, or I will go out and find you. Thank you.

MR. HARWOOD: Thank you, Commissioner Thompson.

(Whereupon, at 12:00 p.m., a lunch recess was taken.)
MR. LIVINGSTON: Good afternoon and welcome back from lunch. My name is Ted Livingston. I'm a consultant who has been doing some work for the Commission in the area of emerging technologies and their impact on consumers and particularly consumer privacy.

My colleague as moderator on this panel is Ellen Finn, who is a staff attorney in the Division of Financial Practices here at the Commission.

Our topic is the implications of RFID use on consumers, and we're really in the next two hours going to try to focus on the consumer and probably not so much on the supply chain, which you heard quite a bit about this morning, and address the benefits to consumers of RFID technology and some of the concerns that consumers may have or maybe should have about the technology, particularly as it relates to privacy issues.

Our goal for this panel is to have it be as much of a dialogue as possible, and with that in mind, we've asked our panelists to limit their comments to five to eight minutes, and we're even calling them comments instead of presentations, so that hopefully we will be
able to finish that part of the panel in about an hour, and then we hope to have a lively discussion and question and answer period for the second hour.

With that in mind, as you know, we have these question cards. If you can put which panelist or panelists you would like the question addressed to, as I think most of you did this morning, that would be helpful, and what we're going to try to do is ask the question of that panelist or panelists and then ask anyone else among the people up here at the table as to whether they would like to comment on that question as well.

So, with that, I will turn it over to Ellen, who is going to introduce our presenters.

MS. FINN: Full bios for all of the panelists are available in your materials, so I am not going to give them lengthy introductions, just a sentence or two each to kind of orient as to who they are as they speak, and rather than go down this long table so that by the time someone opens their mouth, people have actually forgotten who they were, I am going to introduce them one at a time as they speak.

The first person who is going to make a few comments is John Parkinson immediately to my left. He is a Vice President and Chief Technologist for For The Record, Inc.

Waldorf, Maryland
(301) 870-8025
Capgemini's Americas Region and member of the Group's Office of the CTO. In 2004, he was named as co-chair of the ITAA Committee on RFID and the chair of ITAA Task Group on Public Policy Formulation for RFID, and he is going to share some information about some research CapGemeni has done on RFID and his perceptions of it.

MR. PARKINSON: Great, thank you very much. I do need to at least use some footnotes, because I'm a consultant. That's what we do.

So, last year in October we with the National Retail Federation (NRF) decided to try and get some quantitative sense of where the consumer was with RFID, and we did this via an internet panel, which I readily admit already biases the sample, since if you can't get onto the internet, you weren't reviewed for the research, but we asked a fairly structured series of questions about what people understood about RFID, what their concerns were about it, and what they saw as the potential benefits from it, and those results are presented here very briefly.

There is a published report based on this that was released jointly by Capgemini and the NRF, which is available from either of our Web sites, or if you want to see me afterwards, I'll be happy to send you a copy.

The first issue was, why should we worry about
consumers? Almost all of our work today is with manufacturers and the supply chain. The answer is because at the end of every supply chain, there is a consumer, and if the consumer doesn't understand the benefits and the issues around the application of RFID, then some of those benefits won't be realized, and because we believe they are significant to everything up to the consumer and potentially to the consumer as well, we wanted to get a sense of where everybody's head was around this.

This was coincident with the Wal-Mart announcement that got some press release. It was after a number of issues had been raised in the media around the use of RFID tags, particularly post-sale identification tags. So, it's very hard to judge what people really get about this. So, this is why we did the research.

So, what did we find? We found essentially that most people have no idea what RFID is. Not a surprise. It's another of those brand new 50-year-old technologies which is about to roll out into some part of society. So, only about a quarter of the people who were interviewed had any idea.

Now, in the "no, we have no idea what it is," there were a significant number of people who routinely
use either a toll tag or Mobil Speed Pass, both of which are RFID devices, and they had not associated their routine use of those devices with the term RFID. In fact, there were a number of comments that until it showed up on TV, I think they quoted an episode of Alias, they hadn't made the association between the device and the concept.

Men are slightly more likely to have heard of it than women, but not significantly, and people in the survey got their information from all over the place. There was no standard source to go to for reference material.

So, we then said, okay, what do you think about it? And slightly surprisingly -- two slightly surprising things here. One is that most people, the largest single group, had no opinion. So, the second largest group were favorable, which is a broad spectrum of response. Only 10 percent explicitly said that they had an unfavorable view about RFID. So, this is in contrast to some of the material you have seen in the media up until now. And we did find that there was a lot of interest.

So, what were the concerns? Surprisingly, the biggest concern was about the impact on price. This is a new technology rolling out. A lot of people thought
it would put the price of the goods they were buying that were involved in RFID programs, the price would go up.

Secondly, we asked them what they thought the benefits would be, and again, slightly surprisingly, there was a perception that -- again, I think because people think about systems like LoJack, it would be easier to recover stolen goods, and then there was a view that there might be some decreased costs once the supply chain impact had worked its way through, and there was some perception that application to the prescription drug industry would improve safety.

So, when we asked would people be willing to actually buy goods with RFID tags to get these specific benefits, the general view was, "Yes, if," and the "if" was where the privacy issue first raised itself, and the top concerns around RFID cycled back to this issue of privacy, that the data would be available to third parties without permission, that you would be exposed to more targeted direct marketing, which nobody seems to like, and that it would become possible to track consumers via their purchases.

Given how little information people had or understood about RFID, there's relatively low correlation between understanding and the responses to
these questions. There was also some issues about health, which we see show up every time, anything to do with the electromagnetic spectrum it gets raised with, it seems.

We asked if people felt that the RFID issue was greater or less than other kinds of trackable devices or trackable systems, and in general, we got a, yes, we think it probably is pattern of response. Even people who don't, again, necessarily fully understand the technologies that lie behind some things like debit credit cards felt that RFID would be worse than that.

What would you like us to do about it? Let's get some legislation in place that at least tells us what it is people are allowed to do. Let's look at the viability of killing tags post-purchase. Let's look at opt-in/opt-out systems, where at least you could tell merchants whether or not you wanted tagged devices and whether they wanted them killed. And let's at least put a label on the goods and services that we buy that clearly state whether they're tagged or not.

We asked people how long they thought RFID would take to come into widespread use, and generally speaking, people thought five years was about the right number. Only 3 percent said that it would never happen, and that did not correlate to knowledge of RFID.

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
However -- and again, slightly surprisingly -- a much larger percentage said they would prefer that it didn't happen. So, we probably need to go back and do another survey to try and drill more deeply into why there's that contrast between inevitability and desire, and we have some plans to do that.

So, what did we conclude from that? Currently, not many people really know about RFID, and even people who do don't know very much about it. There's a growing explicit interest and growing concerns around RFID -- not all that surprising -- that it would be better we think to communicate more about the reality of RFID to consumers now rather than waiting until it's a more widespread phenomenon, and that education is the route to the consumer mind set, in particular to re-assure them around health issues, to explain that some of the things that they worry about are things that the industry dreams it could do -- nowhere near capable of doing today -- and to help guide the legislative efforts, because from our perspective as an industry, we want to do the right thing to get the benefits from RFID, but we can't yet tell what the right thing is.

The appropriate use guidelines, we would assert, need to be built now so that by the time we have capability, we know we're using it for the right things.
Our concern is that if we as an industry don't do this, then it's likely that other groups with other agendas will.

So, what should we do? Let's look at the sources of insecurity and figure out what we should do about them. Let's as an industry at least get behind the explicit marketing of goods that are tagged, try and disconnect the technology, which is just a technology, from the broader issue around privacy and the use and potential misuse of consumer information and get clear guidelines on appropriate use worked out, and then publish and adhere to whatever those policy guidelines might be.

We need to get moving on this, because the mandate-driven market we have today is moving RFID along much faster than most of us from a technical perspective expected, and we do not want to lose the trust of the consumer in this. We as an industry want to be sure that the consumer knows what they're getting before tags start showing up in places they don't expect.

Now, there's some clear benefit models associated with this, and we'd like to explain those to consumers and let them decide how much of those benefits they want to pay for the price of the goods they buy at retail.
Thank you very much. I will be happy to answer questions later.

Mallory?

MS. FINN: Thank you.

Our next speaker is going to be Mallory Duncan. He has served as Senior Vice President and General Counsel for the National Retail Federation for the past ten years, and he's responsible for coordinating strategic, legislative and regulatory initiatives involving customer data privacy, financial services and consumer protection.

MR. DUNCAN: Okay, thank you and good afternoon.

By way of background, the NRF, who worked with Capgemini on the study, is the world's largest retail trade association. Our membership consists of all formats of retailers. We cover household names, from Saks to Sears, all formats, from a local haberdasher to Home Depot. I am very pleased to be here today.

RFID and EPC are critically important to our customers. As virtually everyone has acknowledged, widespread item-level tagging is still quite a ways off, yet as the Capgemini study makes clear, the privacy implications of tagging seems to be on everyone's minds.

Privacy issues, while potentially significant, are only a portion of the RFID picture. Whether they
achieve significance is dependent upon the handling of
four other issues related to it: Education, notice,
choice and value.

Let me start with just a few observations. One,
individuals are notoriously bad at assessing the
economic value of a new concept in the abstract.

Second, for many, uncertainty is frightening.
Confronted with the unknown, they tend to fall back on
re-assurances, family, home, hearth protection.

Three, in the period before society has an
opportunity to comprehend, experience and reach
consensual accommodation, new technology is often
characterized as creating unwarranted privacy
intrusions.

Now, use of RFID technology in retail stores is
still in its earliest stages. As the study indicates,
most consumers have not heard of the technology, and
those who have, reactions appear to reflect these three
observations.

For example, on the positive side, given its
newness, it's not entirely surprising that consumers
value highly the potential for the technology to satisfy
safety and security concerns, recovery of stolen items,
antitheft capabilities, prescription drug security, et
cetera, and frankly, inasmuch as society still places

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
the bulk of the nurturing burden on mom, these same
family safety potentials might explain why the study
found that women tended to rate the benefits of RFID
slightly higher than men.

Now, improvements such as fewer out of stock,
faster checkouts, were likely ranked lower than
anticipated in the study, because consumers have not yet
experienced the world in which those things happen;
thus, it's difficult to appreciate their value.

Similarly, consumers say they're unwilling to
pay extra for service they can't now imagine. Two
decades ago, if you had wanted to ask consumers how much
they would have been willing to pay for a telephone they
could remove freely from the wall, it's likely most
would have said little or nothing. It's virtually
certain they would not have given a figure comparable to
the $69 per month many cell phone users now pay for that
extra service.

As to privacy, privacy-related questions scored
high in both the unaided and preprogrammed responses to
the study, again, not entirely surprising. When new
technology expands sensory reach, it inevitably reaches
previously ingrained expectations. Individuals react to
change as a privacy violation. Eventually an
accommodation is reached, from which arise new
expectations.

The internet, email within it, cell phones, are all undergoing that process right now. The most famous law review article, "Eliminating the Right of Privacy," published near the turn of the prior century, was written in response to that era's cutting edge technology, telephoto lenses.

Now, let me suggest a proposition. Unless we are aiming to arrest potential benefits, we shouldn't write laws in response to imagined difficulties. Currently, virtually everything about the future of RFID is unsure. We need to see what uses develop, whether where the technology is used in practice falls within or outside of our comfort zones, before we can regulate its use.

An early law prohibiting the photographing of strangers might have stopped peeping toms and killed most photo-journalists. A law making it illegal to telephone unknown persons would have curtailed some telemarketing, but it would have effectively prohibited nationwide public opinion polling and the 911 system.

As technology evolves and technology passes, one can anticipate a more realistic balance between consumer benefits and concerns. Regulations should be considered only if evolving technology use practices fail to meet

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
consumer expectations.

NRF believes that the privacy policy recommendations that our board adopted are applicable here. Our policy recognizes that in a highly competitive retail marketplace, maintaining the trust of one's customers is essential. There may be millions of retail outlets, but in the real world, customers shop at a fraction of 1 percent. For most retailers, repeat business is essential. If a dissatisfied customer walks to another store down the mall, the retailer hasn't lost a sale; he's lost dozens of sales or perhaps scores of dozens of sales.

As applied to RFID, that means that there's a need for education. It's important that consumers learn the RFID basics, its uses in EPC, and receive a realistic expectation of its potential.

Second, there should be notice. The early stages of deployment, when interest in new products is naturally high, is an ideal teachable moment. Currently, a small number of retailers and manufacturers are leading that process. They've begun, but others need to follow. There must be choice.

As with privacy policies, retailers should provide customers with options. For example, they should allow customers to opt out if they do not want to
receive marketing solicitations or have their information for marketing purposes sent to a third person. In some cases, the option, however, would be to choose another retailer.

Information received by a retailer should be subject to reasonable and responsive security and access provisions, and the entire process should be managed with an eye towards value for the consumer. A more cost-effective supply chain is one such value.

As the caption on our research demonstrates, consumers will need to see the benefits of deployment in order to fully appreciate its value. The concept of a Blackberry is not nearly as appreciated as its value.

The potential for overly harsh regulation of new technology is a constant threat. The values of RFID and EPC will only be realized if retailers act thoughtfully, carefully and adhere to the simple principles that have always been at the heart of building customer trust.

Thank you.

MS. FINN: Thank you.

The next speaker we are going to hear from is Beth Givens, who is a familiar face to many people in this room. Beth is the Founder and Director of the Privacy Rights Clearinghouse. Established in 1992, the PRC is a nonprofit consumer education, research and
advocacy research organization located in San Diego.

MS. GIVENS: Thank you, and thank you for the opportunity to speak here today and to participate.

Just a couple of words about the Privacy Rights Clearinghouse, because it will help explain some of the comments I want to make later, we interact directly with individuals. We invite their calls and their emails, and we're kind of the Dear Abby of privacy. We have been doing this now for a dozen years, and quite frankly, we have heard just about everything, although I continue to be amazed and curious about what we do learn about from individuals who are experiencing privacy abuses and problems in the marketplace.

What I wanted to talk about today are four things. I'll first summarize the characteristics of RFID that could threaten privacy and civil liberties, and that will be the focus of my talk. I will follow by critiquing some of the technology-based proposals for mitigating these privacy concerns. Then I'll say a few words about consumer education, something that I think we'll be hearing a lot about today and in the near future. And I'll close by calling for a comprehensive multi-disciplinary technology assessment of RFID.

So, to begin, industry representatives have described many benefits of RFID today, but RFID is a
classic information technology in that there is a potential downside as well. If the technology is implemented irresponsibly, we as a society could experience it not as a wonderful convenience with many social benefits, but rather, as a tool for consumer profiling and tracking. In other words, as one part of a larger surveillance infrastructure. So, the key question is, how do we shape the implementation to ensure the socially beneficial aspects and to prevent the negative ones?

Just to summarize, RFID has several qualities that working together could threaten privacy and civil liberties, and these are, first, the bit capacity of the tags sufficient to uniquely identify all objects on the globe; second, the fact that tags and readers can be installed invisibly, enabling tags to be read from a distance without the individual's knowledge and consent; and third, the database, something that we have really not talked about enough I think, the databases that are developed to compile, store and analyze that vast amount of data gathered as those products make their way from the factory to the point of sale and perhaps beyond.

Now, it's the "beyond" that is of concern to privacy and civil liberty advocates. That's where the item-level data on the tag could be combined with

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
personally identifiable information, at least at the database level. So, put these qualities together, and yes, there is potential to create a comprehensive infrastructure for individual tracking and profiling, something that we want to, of course, avoid.

A variety of technology-based fixes have been proposed to mitigate the potential threats. For example, killing the tags at the point of sale and providing tag-blocking devices to individuals. However, appealing these so-called solutions appear upon first glance, they in my opinion as a consumer educator and consumer advocate are not very satisfying.

Killing tags or blocking them does not address, for example, in-store tracking, and some of the strategies for tag-killing are inconvenient, like killer kiosks, for example, taking your load of groceries over to a kiosk and then de-activating the tags after you shop with two young children in tow and having just spent a hundred dollars to fill up that bag or that cart. My experience as a consumer educator is that these activities will only be used by a small portion of shoppers.

Further, merchants could offer incentives or disincentives to not kill tags, for example, making it more difficult to return or exchange items that do not
have working tags on them. While some might think that
this is unlikely and that the retail industry would not
do this, we only have to look at the present day
situation around product returns to realize that it's
really not out of the picture.

I mentioned that we have been talking with
consumers for a dozen years now. Consistently, year
after year, in the top ten of our complaints are
complaints about merchants who require individuals, when
returning items with a receipt in hand, to provide name,
address and driver's license number. Otherwise, they
cannot return those items. This is not an unlimited
practice. We've got in our database the names of all of
the major retailers in the U.S. So, this sort of thing
could happen with RFID, kind of a disincentive or
incentive to keep those tags working.

Disadvantages that I see for blocker tags are
that they, like the killer kiosks, add a burden to
consumers. They fail to protect consumers when those
products are separated from the blocker tag, and like
the kill choice, they create two categories of
consumers, those who take the time and energy to
deactivate and the larger number for whom deactivation
is inconvenient or is without meaning.

Industry representatives are calling upon

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
consumer education as an important way to mitigate consumers' concerns and to instruct individuals on the choices that they have to protect their privacy. As a consumer educator, I take this recommendation very seriously. It strikes very close to home, and I think it's very important to differentiate between a true consumer education campaign and a public relations campaign. There's a big difference between the two of them, and let me give you one example of a consumer education campaign that I was involved in many years ago.

In 1996, we at the Privacy Rights Clearinghouse participated in a comprehensive consumer ed campaign revolving around Caller-ID in California. The message of consumer choice revolving around which blocking option, a comprehensive blocking or selective blocking of your phone number as it goes out over the wires, was basically the message that needed to be transmitted to Californians.

So, the message was developed by a committee that was comprised of representatives of all stakeholders, the phone industry, the regulators and the consumer advocates, and that message was not finalized until we could all agree upon it, and that message was ultimately conveyed by multiple media, TV, radio,
newspapers, and in many languages.

By the time the Caller-ID was launched, a survey was done, and it showed that two-thirds of consumers were aware of their choices, and the effort was guided by an academician, who was a communications scholar from Ohio State University, and her expertise was in the area of public information campaigns. So, that is what I would call a consumer education campaign.

In convincing with the consumer ad initiative for RFID, I strongly recommend the development of strategies borrowed from such efforts as I just explained.

Now, last November, 50 consumer, privacy and civil liberties advocates got together and released a position statement on RFID. That was led by CASPIAN, the Privacy Rights Clearinghouse, along with EPIC, EFF, the ACLU and others. You can find that statement on our Web site, privacyrights.org, as well as several other Web sites.

We call for the implementation of RFID to be guided by the Fair Information Principles, something I will not talk about now because it will be discussed later, but what I do want to spend just a few moments on is what we called for, which was a comprehensive technology assessment to be conducted by an impartial

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
body or group of impartial bodies, akin to the type of assessments done by the Congressional Office of Technology Assessment that existed from '72 to '95.

Even though industry is moving full speed ahead with RFID, I continue to believe that such an assessment is vitally important for the responsible implementation of the technology. Ideally it would consist of a multi-disciplinary analysis covering the expected benefits as well as the expected adverse impacts. It would include not only privacy and civil liberties, but also labor impacts, which I think are going to be huge, environmental health implications, and of course, what we're talking about here today, which is privacy.

It would be overseen by an impartial body, perhaps a body like the Federal Trade Commission, the National Academy of Sciences, an academic institution or perhaps working together as a consortium, but "impartial" I think is the key word.

Just let me throw out two or three questions that could be addressed by a technology assessment. One would be what would be some of the unintended consequences, something we oftentimes learn way too late.

Second would be are there other technologies that could do some of the same things but are less...
intrusive, and I think Intel brought that up today with
the discussion of 2D bar codes.

Then third, do we need to have all of these
items in the world uniquely identified? Could radio
frequency identification work well with just a bar code
level being emitted, generic information? For example,
bringing your computer to the landfill. It doesn't have
to say, "Lead inside, and this lead belongs to a
computer that was paid for by Beth Givens in August 1983
purchased at Circuit City." It could just simply say
"lead inside" or "mercury inside" or "nickel cadmium
inside." So, there could be an RFID implementation that
is not quite so intrusive as the EPC.

One of the aspects of Congress' technology
assessment that I liked the best was that it came up
with not one policy solution but several, so that
lawmakers, industry and others could see different
scenarios based on, say, low regulatory environment,
moderate or high.

In closing, I strongly recommend that the FTC or
perhaps the National Academy of Sciences, a scientific
or academic institution or even a consortium approach
take this approach. Now, we've already got several
pieces of a technology assessment in the works,
industry, some academic institutions, consumers groups.

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
I think we have a good start, but we need that impartial look at this technology.

With that in mind, I close with a quote from Senator Patrick Leahy, and I think he wraps everything up that I said quite nicely in one sentence. He said, "We need clear communications about the goals, plans and uses of the technology so that we can think in advance about the best ways to encourage innovation while conserving the public's right to privacy." He said that in March of 2004.

Once again, thank you for the ability to participate today, and I'll look forward to the questions and discussion.

MS. FINN: Thank you, Beth.

The next person who will speak is Deirdre Mulligan. Deirdre is Acting Clinical Professor and Director of the Samuelson Law, Technology and Public Policy Clinic at the Boalt School of Law at the University of California, Berkeley, and she came to Boalt from the Center for Democracy and Technology, where she worked on privacy and free speech issues.

MS. MULLIGAN: Thank you. It's a pleasure to be here this afternoon.

I run a clinic, as she mentioned, which is kind of the lab component of law school, and so students both...
from our computer science, information sciences and from
the law school work with me on different kinds of
projects. Some of them might be actual litigation or
legislative activity, and some of them are more
research-oriented.

We have been engaged in a variety of
research-oriented activities around RFID and more
broadly what we call pervasive computing. I believe Ken
Fishkin mentioned kind of pervasive computing. We've
heard sensor networks thrown out. So, the notion that
computers are going to be embedded into our physical
environment in so many ways, in the virtual world, where
people are concerned about cookies and people tracking
what they do online all of a sudden meets the physical
learn, where the kind of tracking that we've only
imagined occurring online is now embedded in the world
around us. So, they're not tracking your clicks;
you're now tracking where we go.

I think Ken Fishkin had some really elegant
elements of the kind of neat things we can do, the
invisible man or the invisible woman, you might say, but
there are also some real privacy concerns.

I remember being here in 19 -- I don't know,
maybe '95 and then Chairman Pitofsky talking about they
don't only know online that I chose the salmon, they

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
know that I considered the beef, right, and so there is
an awful lot that we can infer from the use of this
information.

We have been particularly focused on a very
special kind of good, and that good is information
goods. Information goods, books, CDs, DVDs, all that
intellectual property that we hear about, they play a
very special role in our society, right? We have
protections stemming from the First Amendment and the
Fourth Amendment that protect governments from trying to
get a hold of what it is that we're reading, right, so
whether it's limiting government access to records that
might be held by a bookstore about who's purchasing
books -- you will remember the Monica Lewinsky and
Kenneth Starr debacle here at Kramerbooks -- so there is
some Constitutional protections.

In the absence of Constitutional protections, we
have had Congress repeatedly step in and say, well, even
where we might not have a Constitutional issue, we're
very concerned about the freedom of inquiry, right, as
we see it as the corollary to freedom of speech. If all
of us can speak but the government is kind of then able
to see who's kind of listening to whom, we are going to
have this chilling effect, the same way we might if
everyone was forced to disclose who they were before

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
they entered the great marketplace of ideas.

So, people often talk about privacy law being very patchwork and unsystematic, and in fact, when we talk about information goods, Congress has stepped in pretty frequently, and there is the Bork -- during Bork's confirmation hearings, people may remember this, an enterprising reporter at The City Paper here in D.C. got hold of Judge Bork's video rental list and said, oh, nothing interesting, but people on the Hill said, oh, could have been something interesting, right, so we have the Video Privacy Protection Act passed which provides a protection for our private viewing habits. We have rules that protect cable viewing.

At the state level, dealing with libraries, I think it's 48 states -- and there's probably a librarian in the room who will correct me -- but I think it's 48 states have state legislative protection around librarying of patron records. So, we have a very rich culture of protecting the privacy of our freedom of inquiry, what it is that we're accessing.

The good news is information goods providers generally are into this culture of confidentiality, right? So, book stores oppose subpoenas that are overbroad that they think are inappropriate. Libraries have very strong kind of, you know, their Constitutional

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
kind of principles that protect privacy.

So, what does this have to do with RFID? It was mentioned earlier that libraries are implementing RFID systems. There's been a lot of focus on libraries. I think it's good to kind of step back, and libraries, as I said, have this very strong culture backed by state law of confidentiality protections. Most of the other retailers that deal with books do not, right, and so certainly many of them step up to the plate in the context of books and protect privacy when a government subpoena or private subpoena might come around.

When we talk about introducing something like RFID into the mix, it gets a little bit more complicated. So, we have some threats that I think are important to think about.

RFID, as I mentioned, it works on a broadcast, right, so my RFID tag is talking to everybody, this word promiscuous, which I have a really good slide in a little bit to talk about promiscuous tags. There is no access control on this. We can't even think about eavesdropping, because the whole intent of the technology is to let everybody listen. So, depending on what is embedded on that tag, right, we could be overhearing lots of different things.

People have talked about tracking point to
point, all right, so we can track as an individual moves potentially, but I think also, interestingly, we can track as a good moves. So, if I know that Deirdre purchased a particular book, we can now figure out who it is that Deirdre is lending things to, or if we've decided that a given person who we've decided is suspect has a certain kind of good, we can look for other people who might have that kind of good, and when that good happens to be a book or something that is about our inquiry, I think that that kind of tracking raises particularly, you know, troublesome concerns.

Beth mentioned the invisibility of the tags and readers. We've talked a little bit about joining data. I want to look a little bit -- there are some real important differences between the RFID technologies being deployed in libraries and the RFID technology that we're talking about, primarily EPC standard, in the general commercial space.

Libraries, as I mentioned before, you know, they really live and breathe privacy. Many of you are probably familiar with the whole debacle around Section 215 of the Privacy Act. Libraries are very, very concerned about Attorney General Ashcroft coming in with subpoenas that they can't talk about for people's borrowing records.
So, if you look at -- the most important differences here, the read range, right, library read ranges for the little tags that we have are one to four feet, pretty close proximity, versus the EPC tags, 20 to 30 feet, you know, depending on the environment. The labeling protocols, in the library setting, there isn't a standard, and there's not a standard for the technology. There's a bunch of different standards that are out there, and some of them are proprietary and not really standards, and there's also no labeling protocol. So, libraries are doing different things. They tend to be library-specific. So, it's much more difficult to correlate, well, you're borrowing this book, and so this book over here that has the same identifier must be the same book. It doesn't really work that way in a library setting.

In EPC, with this 96-bit globally unique ID, you will see we have a slightly different picture potentially. So, here are the two books, and I love -- these are my promiscuous tags -- I'm sorry, I just had to do that -- so, in the EPC version, the tag might actually be saying something like, you know, this is a Penguin Publisher, it's Catcher in the Rye, and this is copy 51034. Now, if that, in fact, is what's being broadcast, I think many people would find that quite out
of sync with their own expectations of, you know, who's
going to have access to what they read. In the library
setting, it's more likely to be this string that doesn't
necessarily add up to anything much.

Now, we've had a little bit of a conversation
about the back-end databases. Part of that depends upon
what this tag points to and what kind of access controls
are on that tag. Somebody stated earlier, I think it
was the first -- Sue Hutchinson, I think was her name, a
woman who spoke early this morning -- and she said that
all of these servers are sitting behind firewalls at
companies, and I actually don't think that's going to be
the case. I think that there are going to be all
different kinds of servers.

Many of you are probably familiar with the
internet movie database where you can go and look up a
movie. You can certainly go in some libraries and using
the ISDN number get to a book, right? So, you can use a
number to look up the content. We are all very familiar
with reverse lookups with phone numbers. It used to be
I could only look Beth up by her name, now I can look
her up by her number and get her name. And here, too,
depending upon the availability of the databases and
what kind of access we have to them and how centralized
they are and what their rules are, we can have very
different things coming out of both of these contexts.

So, I am going to end with some conclusions, solutions and recommendations. I think that, you know, with respect to information goods in particular, RFID does pose a substantial privacy risk, and what's important I think from the FTC's perspective is that I think it does violate established public policy. I think people have very deeply ingrained, legally protected in some instances, collectively shared expectations that the books that they borrow, the books that they purchase, the movies they watch in their house, that there is some privacy protections that people aren't able -- you know, I take the book, I buy it, I put it in the bag. I don't want the book talking to other people and telling people what I'm reading. If we don't think about that when we're deploying the technology, there's a potential to run right into those in a way that I think people would really find very unfair.

Many of the solutions that have come out are either inadequate or they're not particularly useful in the context of information goods. Information good markets are different. They don't tend to be like the sweater that I buy and eventually it falls apart and I ditch, right, or it ends up in the -- books tend to revolve in the marketplace. We have many lending
institutions, not just libraries, but video rental, you
know, we have much more of a culture of exchange, and
people also tend to collect and archive.

If you remember the CueCat device, which was
sent out -- I don't remember which business introduced
it into the market, but you could take it and we were
all supposed to get our magazine, wave the little CueCat
and be linked to a Web site that was going to market to
us, and some good engineers decided to hack into it,
reverse it and use it to catalog their CDs and catalog
other things that had these little bar codes on them.
And consumers are very interested.

There's a whole bunch of software programs out
there, all different kinds of things that help us
archive our collections. So, I actually think that
there are some interesting consumer end uses for RFID,
but I certainly know that to the extent that we have a
revolving market, we have book stores that are both new
and used, we have people who routinely sell books back,
that killing tags doesn't necessarily kind of fit in
that kind of marketplace. It sure doesn't work in the
library setting.

I do think there's a role for the FTC. Beth and
some other folks have spoken about a formal technical
and policy assessment of RFID technology. I'm doing

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
that now, and I think that it would be really nice to have a formal process rather than the ad hoc process that we have going on in various areas.

I do think that it's really important when we're looking at technology not to say, oh, any law is bad. In fact, I think RFID, and there's been a host of other technologies, we've actually shied away from some of the more interesting potentially innovative uses, because researchers get anxious because, oh, when we're dealing with people, we have these privacy concerns. Let's track the trees. Let's look at the ducks. Let's stay away from the people.

There's a missing piece that law, in fact, can be enabling. Law does not need to be something that, you know, that kills technology. That's just not at all the right way to look at it.

I do think that information goods tags, when we're talking about information goods, RFID tags I really think we need to be considering that there have to be limitations on what they can reveal and how easy it is to get from a tag to databases that tell us what people are consuming -- I hate to use that word -- in relation to books and music.

With that, I will close.

MS. FINN: Thank you, Deirdre.
The next person who we'll hear from is Dan White. Dan has one of the more interesting job titles I think I have ever encountered. He is a technical evangelist, RFID, in technology for NCR's Corporation's Retail Solutions Division. Dan's responsible for evaluating RFID and other new technologies, determining potential applications in the retail industry and formulating strategic direction relating to these technologies.

MR. WHITE: Well, as I've been sitting here listening, I was thinking as a consumer, why would I want RFID? What is the benefit to me personally? As I look at it and I think about what might be going on in the future, to get to the most basic level, RFID lets you find things. So, I think about five years from now, I might be sitting behind the TV looking at late night TV and see an infomercial saying, buy this RFID tracker, it will help you find your keys, it will help you find the remote control that you're missing. It might even help my wife keep track of the tools that she borrowed so that I can find them after she borrows them.

As I was growing up, one of the things that always amazed me was my mother, and she always bought things on sale. Whether or not we needed them or not, she bought them. In fact, one time she bought five
boxes of corn flakes, and so we ate corn flakes for seven days for breakfast, lunch and dinner, and as I was thinking about the things she used to do, one of the things she did was after Valentine's Day, she would buy candy, and she would buy it for, you know, Easter or Christmas. So, I don't know why as a child I always wondered why the Easter bunny, you know, left me Valentine's candy, but she did it because it was on sale.

The problem came about was we never had enough storage. So, she would end up hiding things. Number one, she hid them so we wouldn't find it, but the other reason was so that she could actually get to it when she needed to. Inadvertently she would forget when she hid them, and yes, one Christmas, I had Valentine's candy, and we weren't sure which year it was from, so I still check things when I go home and make sure the expiration date's not gone, because she does seem to hide things. So, whether it's something you've hidden in your home or something that you may have lost, RFID in the future may allow you as a consumer to be able to actually find things that you're looking for.

If you take that concept into the store, and a lot of that's been mentioned this morning, finding things in the store is very critical. You may go
shopping in a clothing store, and how many times are
things put in the wrong place? Being able to know where
it is at any one time in the store is powerful for the
retailer. It's powerful to let them know exactly where
it is at any one time.

If they're out of stock, like they've been
talking about this morning, they can go get more and
refill it, because the key thing in retail is if you
can't find it, you can't sell it, and from a consumer
standpoint, if we can't find it, we're not going to buy
it. That's why this is such an important technology to
the retailers.

If they're able to find it not only in the store
but all the way up the supply chain, you can imagine a
few years from now, you'd be able to go into a store, go
to a computer and say, I want this particular size in
this particular style of pants. They would tell you
exactly where it is, that it's in stock, and it might
even light up and say, "Here I am," so you don't have to
go through the rack of clothes. To me, that's a lot of
benefit. I hate going through a stack of clothing.

Looking forward, some of the things also, it's
not just finding things, but a lot of the benefits that
the retailers have been talking about are actually
lowering their costs. This was mentioned briefly, but
if you look at the supply chain, it makes them more
efficient, and it means they can reduce their inventory.
All of these things ultimately will lower their costs.
It's not near term, it may be 10 years, may be 15 years
from now, but their lower costs will be passed on to the
consumer. So, from a consumer benefit standpoint, we're
going to be able to find things better, and we're going
to lower our costs. Those are some of the key benefits.

I think there's a lot of valid points that have been brought about today, and as we start looking at
them and start having discussions about what are the
issues, I think we need to be very honest and open.
Some of the policies that have been put in place are
providing information in an open manner. We don't need
to hide anything. We need to say exactly what the
technology can do, and instead of being PR, we should be
also telling what some of the concerns are, and let the
consumer decide.

I think ultimately, the best benefit the consumer can have is have the ultimate decision in
knowing what they want to do with the technology.

Thank you.

MS. FINN:  Thank you.

We'll now hear from Sandy Hughes. Sandy serves
as the Global Privacy Executive or GPO at the Procter &

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
Gamble Company. She also founded the Council of CPOs for RFID Electronic Product Code Pricing Implementation, and she's a member of the Public Policy Steering Committee of the EPCglobal, and she's been active in creating guidelines and is a speaker on the use of item-level tagging.

MS. HUGHES: Thank you, Ellen, and thank you for the opportunity to be here.

I hope some of you are familiar with Procter & Gamble brands. We have over 300 in 160 countries around the world, and we have 13 that have over a billion dollars in sales each. So, if you look at this picture, hopefully you use some of those. Can you tell me which one is missing? It's the one that's out of stock 8 to 12 percent of the time.

For us, we are interested in EPC, as you've heard, because for us, it's about putting the right product in the right place at the right time and at the right price. For us at Procter & Gamble, the consumer is boss. That's a mantra that we carry throughout all of our interactions, in everything that we do and what we create, and the potential we feel for EPC is throughout the entire supply chain, between us and our suppliers, through the retailers, to the consumers, through managing inventory, preventing theft and

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
counterfeiting and reducing out-of-stocks.

Now, at Procter & Gamble, we are focused on the supply chain. We haven't even begun to think about what's going to happen post-sale for item levels that leave the store, and for us, what's important, though, is the way the consumer is feeling, because as I mentioned before, the consumer's boss, and the way that we manage the first moment of truth, what they see on the shelf, really impacts whether they pick us up, they continue with us, and continue as loyal consumers.

We have plenty of issues and things before we are able to adopt EPC throughout our company. We are a global company, and therefore, every solution that comes up has to be a global solution, and this means across all product categories and across all countries. In technology testing, for example, we've heard about some of the limitations when you think about liquids and metals. So, in the testing that we have done, looking at paper products, we have no problems with reliability. You start to look at Pantene or liquid-filled items or even our Cascade that has metal on the cases, on the products, we have more difficulty.

But as I mentioned, we're looking at supply chain, and we are able to pretty efficiently read labels, tags on cases as they go sequentially down a
conveyor belt, also on pallets, but when you get to mixed cases on a pallet, we have a long way to go there, and the cost is really important. If you think about a 99 cent can of Pringles and then putting that in a case, when you get to some of the prices that we've seen for tags in that whole process, it gets to be something that we have a lot to work on.

The supply chain and internal adoption, within our own four walls, we have incremental benefits, because the state of our computer systems are pretty efficient as they are. So, this requires collaboration throughout the entire supply chain with retailers for us to realize any additional benefits, and that means with all retailers. We don't want to have a set of standards and ways of doing things for one retailer versus another retailer or in one country versus another country. So, for us, being a global company with global processes, we need a global solution, which brings us to the standards.

We have heard some of the difficulties in, you know, different countries, standards on spectrum, on, you know, how the actual coding is done on the tags. We are working very closely with EPCglobal on a number of different task forces to come up with standards that work across the whole broad range of issues for us.

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
have some products with EPC tags and some that are not and different standards is just not cost-efficient for us.

And then finally, public understanding. Even though we are focused on the supply chain, we realize from all of the research and some of the media articles and the things from our own hands-on studies that show that RFID is a concern to consumers. As I mentioned, this is very important to us, and balancing the benefits that they will get with solutions for privacy, health and safety, et cetera, is really important to us. I think the solutions are really going to be a combination of technology, business processes, guidelines, accountability, and we've been able to do that with our consumer marketing.

Let me talk to you a little bit about our Global Privacy Program. Our objective is to create an environment of trust and confidence where consumers or anyone that we do business with or collect personal information from will willingly share their information so we can better meet their needs. And if we want to delight the consumer and have them be our boss, they need to tell us what they want. So, we need to develop that level of trust.

We have a global principle that we will treat an
individual's information that they give to us as if it were our own. We follow the fair information practices of notice, choice, security, access, children, et cetera, everything across the board in all countries, whether there is legislation or not, and we also do it across all media, so whether it's online, offline, wireless and now RFID, and that is for across all constituencies, whether it is consumers, consumer marketing, consumer contact centers, employees, shareholders, recruiting, et cetera, same principles, same objective around the world. So, we need global solutions.

Some of the successes we've had in this consumer trust is that we have recently been voted by consumers, over 6000 in the United States, as being the number one consumer products company for ensuring consumer trust and privacy. We were number three overall, behind ebay and American Express.

The other thing is that a lot of people feel that privacy policies and statements are not read on Web sites and online. We have found this not to be true. Over 4 percent of the hits to our pg.com are to our privacy statement.

We are a permission-based marketing company, and therefore, any further communication that we would have
with a consumer is an opt-in basis. We have over 2
million subscribers who are providing their information
about their children to our Pampers newsletter so that
we can follow the development of their children.

A similar situation with our homemadesimple.com,
which is a program for making your work life balance
more efficient, where you share information with us and
we're able to provide products and services and tips for
you. We have less than 1 percent who opt out. So, we
have seen a number of successes, and I feel this will
happen with RFID as well as just a new technology to
consider for privacy.

How does that come together? We have on our
company Web site a privacy page where you can see our
policy, our privacy statement. We do have a short
notice up there, so you can go out and see it at a
glance under Policy.

We also have a position statement on electronic
product coding that says that we require notice whenever
tags are being used, choices for consumers, education,
and if there is any retailer or partner that we're
working with that would be using personal information
together with tags other than they do for bar codes
today, then we simply won't work with them if there is
going to be any type of item-level testing.
We also have education, as we talked about, which is very important for consumers, privacy news, and the last thing is where we are actually testing the technology. As I mentioned, it's pallet and case, but in the example of the Wal-Mart test, where there is even the potential chance that there could be a case that would be on the floor, even though it shouldn't be, that a consumer could buy, we have even gone to the extent of labeling all cases, whether it could be on the floor or not. So, we are not doing item-level testing, we are not putting it there, but just in case it could be, we have labeled every case. So, we go a little bit overboard that way to ensure consumer trust and loyalty.

Thank you.

MS. FINN: Thanks, Sandy.

The last person on the panel is Bill MacLeod, last but not least. Bill heads the competition practice of the law firm of Collier Shannon Scott in Washington, D.C. He specializes in antitrust, advertising and trade regulations, and his practice ranges from the FTC to Department of Justice, Congress and the courts, and among other things, a variety of positions he has held, he was the Director of the Bureau of Consumer Protection here at the FTC from 1986 to 1990.

MR. MacLEOD: Well, thank you very much. Thank
you for having me here today.

I thought it would be a good opportunity now at
the end of this session for me to wrap up with a couple
of observations, both about the promises and about the
corns for RFID. We've heard a lot of both, and I
think we're here at the ideal setting to the consumer
for both, because what we are talking about as far as
the promises are concerned is whether the marketplace is
going to accept RFID, whether the marketplace is going
to acknowledge that the benefits of RFID outweigh the
costs.

We've heard a lot of potential for how those
benefits can, indeed, deliver new value throughout the
supply chain and perhaps beyond. The ultimate test for
that is not going to be decided here, of course. It's
going to be decided out there in the marketplace when
companies do determine that the benefits of RFID do, in
fact, outweigh the costs.

Where are the concerns coming in? The concerns,
of course, are concerns about consumer protection, and
that brings us back here again to the Federal Trade
Commission, the federal agency primarily concerned with
consumer protection in the United States, and the beauty
of being here at the FTC is we have the agency not only
that covers consumer protection, but the agency that

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
appreciates the need for the marketplace, to sort out
the winners from the losers.

What I find especially disconcerting perhaps
about the conversation so far today is a
misunderstanding of how the FTC law and FTC law
enforcement has evolved over time. We haven't heard it
directly from the panelists, but we have seen a lot of
literature and a lot of releases to the effect that we
are sailing without specific protections here. We don't
have any laws in place yet with the words "RFID"
encoded, and what does that mean for consumers and
whether or not they will be protected from the new
forces that this technology will unleash?

Well, the answer from the FTC standpoint, at
least if the FTC approaches this as it has approached
most things in the last 90 years of its existence, is
that you don't need "RFID" drafted onto Section 5 for
the Federal Trade Commission to protect consumers from
potentially unfair or deceptive practices that could
occur as a result of RFID.

The Federal Trade Commission has been protecting
consumers from deception and unfairness since before
we've had TV, almost before we had radio. Section 5 was
not amended when radio came along. It was not amended
when TV came along. It was not amended when computers
and email and everything else came along. Certainly there have been some specific statutes enacted in the past and some regulations the FTC has adopted to deal with particular aspects of emerging technologies, but by and large, you will find the FTC enforcement in most consumer protection to stem from the basic protections of deception and unfairness, and privacy is no exception.

Much of the privacy agenda at the FTC developed after I left. I had the fortune or misfortune, as my client might think of it, of defending one of the first cases the FTC brought for privacy protection involving children. I won't mention the name of the client, for which I am sure I will be appreciated, but the issue was this. It was the releasing of personally identifiable information or at least the making available, whether it was released or not, of personally identifiable information, and the FTC proceeded on the basis of its deception doctrine because the company had a policy in place already that said we will not share, make available or otherwise release personally identifiable information about the children who visit our Web site.

That very policy has informed most of the law enforcement cases we have seen so far, whether it is a violation of a stated policy or especially if you go out
into the states and into the class actions, you will find violations of unstated policies, failures to disclose that information has been made available or has been shared with other marketing partners. These cases have been brought by the Federal Trade Commission, other consumer protection agencies and plaintiffs' class action lawyers without the need for a single additional piece of legislation.

The RFID I think will present something very little different as far as the protections that we need to see and at least as far right now as we can see of what the technology is promising us today. The consumer implications of RFID are pretty clear from the presentations we've heard today. It has the potential to lower costs. That is a potential that can be worked out very readily in the marketplace between retailers and suppliers, something the consumers will simply benefit from as a result of the marketplace delivering those costs through competition in the form of lower prices to consumers, but what will happen if and when some of the concerns we are hearing about come up?

My suggestion to you is that the first line of defense will once again be the Federal Trade Commission, as it has often been in the past, in applying its Section 5 authority and stopping a company from

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
violating its publicly stated privacy policy, stopping a retailer from violating its publicly stated privacy policy, and you can probably bet that there will be Federal Trade Commission cases, if not class actions and state attorney general cases, against abuses of RFID technology long before there is ever a law that mentions RFID.

I remember in one of my prior jobs before I was here at the Bureau of Consumer Protection at the FTC, I brought a case against a manufacturer of cable decoders, pirate cable decoders, using the unfairness authority of the FTC. It was a somewhat controversial case here at the FTC, because it was a novel application of the unfairness jurisdiction, but no one said to me, Bill, the FTC Act doesn't say anything about cable decoders. It doesn't have to. Unfairness and deception or to protect consumers from unfair deceptive acts and practices, whether it's computers, decoders, books, information goods, consumer product goods, it doesn't matter. The Federal Trade Commission Act can protect us.

How many of these concerns do we ultimately hear will ultimately become realistic concerns? I don't know. Some of these remind me of the comment that one of our famous presidents, not President Reagan, once

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
said about his economists. "I remember this economist, he predicted nine of the last five recessions." There are undoubtedly going to be some concerns that we need to take into account, but we need first to identify which ones are realistic and which ones are not.

I think you all might have seen the stories over the last couple of days of these new private companies that are about to launch people into space. I don't think we have to worry yet about getting a conference together to determine whether or not they are going to sell tickets fairly and at reasonable prices. That's getting a little bit down the road.

Why don't we similarly wait here and find out whether there is going to be a concern that legitimately arises as this technology develops and then ask the question whether this is a concern that is a concern that cannot be addressed with the application today of unfairness and deception under the FTC Act, and then we will know the answer to the question whether or not we need a legislation or a regulation that says, "RFID needs to be regulated the following way."

I can tell you one thing both from my experience as a regulator and my experience defending people against regulators. I have yet to find a target of an FTC action and I have yet to find a client of my own who
thought that a law was enabling, was a freedom-giving experience. When someone gets sued for violating a law, I guarantee you that is a restriction that stops activity. If that activity is the activity you did not mean to stop, the law was a mistake. Let's let the law develop where and when we know it needs to be developed.

Thank you very much.

Mr. Livingston: Okay, that completes our comments and presentations. If any of you have questions, there will be people from the FTC coming around picking them up.

While we're waiting for those, I have a couple of questions I'd like to ask, actually a couple of conundrums that I'd like to explore with the panelists. The first one is really for anyone, but maybe Mallory and Beth and Bill could comment on this one. Everyone we've heard from today agrees that item-level tagging of most consumer goods is ten years away or maybe even more, yet RFID is a consumer issue and some would even say a high-profile consumer issue today, as reflected in media coverage. It's really a two-part question.

If there is a disconnect between these two pieces of information, why, and probably more importantly, what can or should industry, government, For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
advocacy groups and others do to bridge the gap between reality and perception?

MS. GIVENS: Well, I think that's why I'm so -- why I recommend that a formal technology assessment akin to what the Congressional OTA used to do is so important. I think we should, as experts, be looking ahead.

I disagree with Mr. MacLeod saying let's wait for the problems and then figure it out. I think, you know, we're experts here. Let's take a look at things that we've experienced throughout the years and maybe apply some of the lessons to what we see as really a revolutionizing technology, a technology that obviously has tremendous benefits for many people in society, yet as I said, like a classic information technology, it also has that downside, something that needs to be mitigated, and I think by some decent analysis and planning and surveys that are done -- I think we need more research that's done by impartial bodies so we can get a sense of what consumers really are thinking about this.

So, I think we should really look ahead with all the knowledge that we have and the experiences we've gained over the past and try to mitigate the potentially bad things that could happen.

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
MR. DUNCAN: If I may, the honest answer I believe is that because people like to dream, you could look back at Jules Verne, look at the old Buck Rogers serials, and lots of fantastic inventions were thought of 50 or 100 years before their time, and yet none of us would think, let's go out and regulate, make sure that doesn't happen.

I mean, the fact is, this is a relatively new technology. In people's minds, it's very open-ended. It's, in fact, technologically quite limited. So, we need to find what the technology can actually achieve before we put the brakes on.

MR. LIVINGSTON: Anyone else down there want to --

MS. MULLIGAN: Actually, if I could, I just want to build off of Beth, you know, that this is the time to think about it. You know, misinformation and myths flourish when there is not an adequate record, and I think this particular proceeding is a really important part, but I think, if anything, as information begins to trickle out, unfortunately, I hate to say this, but you know, I believe Ken Fishkin came and gave us this really cool, "the invisible man," and I can just imagine some of the stories that are going to happen, you know, Intel is going to place chips in everything, right, and you
know, that's not what I'd want to see happen to it, but in the absence of kind of big thinking, deep thinking, people are anxious, and when people are anxious, you know, you get stories, some of which are crazy and some of which are, you know, dreaming, and some dreams come true.

But I also wanted to say that, in fact, industry has supported legislation in areas and they have viewed it as enabling. I would say the E-Sign Act would be an example, I would say the Electronic Communications Privacy Act. There have been numerous areas where industry has decided that privacy legislation would, in fact, be enabling of technology, and some of your clients I guess are supporting that legislation, because some of the biggest technology companies I know of did.

MR. MacLEOD: Let's talk for just a second about the need for impartial bodies. Obviously we have a great ability here hosted by the FTC to have some folks that are partial about the technology and partial against the technology, letting the marketplace of ideas work out what is the best and what is not so good as far as RFID is concerned. There's nothing wrong with partial bodies.

What if we had an impartial body at the time that VHS and Betamax were fighting it out and the
impartial body had picked Betamax? The marketplace is the best place for us, first of all, to determine which is the best technology, and then it's going to be the job of the sponsors of that technology to sell it to consumers, and if they fail, the consumers are going to abandon them, and we are not going to have to worry about any sort of legislation about RFID, because consumers won't want it. The marketplace first has to decide, and then we can determine whether or not there's something more for the legislators to decide.

MR. LIVINGSTON: Okay, here's another possible conundrum, and I'll address this one to Dan and anyone else who wants to talk to it.

It seems that a flash point for RFID relates to how the data is collected. There's a fear that it will be collected automatically and without the consumer's knowledge. Is this really the crux of the issue, or is it what is done with the data regardless of how it is collected?

MR. WHITE: If you're looking at EPC tags today, it's been stated it's just a number. I really think -- and Beth mentioned this -- I think one of the key areas we really need to look at is what you do with the data and how do you manage that.

If it's actually captured and nobody can
associate that with anyone, there may be some concerns, but I think most of them probably go away. So, making sure the data is secure, that if there is any way to associate that with an individual, that that's managed in a way nobody can get at it that shouldn't, and putting in the protections for the consumer there.

I think there's a lot of discussion that needs to happen there. A lot of it's already occurred in other data management type situations, but we may be at another level now that we're talking about being able to track after the fact.

MR. LIVINGSTON: Any other comments on that question?

MR. PARKINSON: To a large extent, this isn't just about a technology. It's about the technologists. There's a lot of things that we can do today that we don't do because there is no profit in it. The market won't allow profitless services to develop for very long.

One of the threshold factors around RFID, there's a technical challenge for us, is what do we do with all the data? Not good things or bad things, just do with it? A fully instrumented economy today would generate 30 terabytes -- to use a technical name for a lot -- of data every day. We don't have any place to
put that today.

So, what we're going to do with it likely, what we did with credit card information when that system first started, we are going to throw most of it away, and most of it isn't very interesting. Most of it's picked up, dropped off, okay kind of data. Only when it gets to the customer interface and we can actually start associating across databases does a major concern arise, at least from my perspective, and that is a very technically challenging thing to do today, except in special cases, and to do it generally probably is beyond our ability to afford for quite a long time.

So, it's always difficult to generalize from proof of capability pilots into general deployment, and what's really challenging everybody today is figuring out how to perform general deployment, even if competent.

MR. MacCLEOD: There is a capability today and the information exists today that someone can make a great deal of money selling. Every time I shop at Safeway, every time I shop at CVS, I run my membership card through the scanner. Safeway and CVS know a whole lot about my habits, and I guarantee you if they try to sell that to anybody, that is almost certainly going to get out, and there are a number of law enforcers in this
room who will give them the misery of their corporate lives, and what RFID is doing is simply providing a different way of gathering information that can be misused or can be used properly just as the information that is being gathered today. It is the conduct that we have to worry about, and it is the conduct that is already being protected by the privacy policies announced by retailers and by the law enforcers and by the plaintiffs' lawyers who will make it very painful on anybody who violates those promises that they have made to consumers.

MS. FINN: I'd like to ask a question, and maybe Beth and Sandy, you'll want to comment on this or anybody else who wants to jump in.

We've heard a lot about the supply chain and a little bit less about some of the item-level tagging applications and what that may mean for consumers and some of the applications that may benefit them if they leave these tags enabled, you know, along with presenting in terms of, you know, monitoring something that you want to take, to raise the possibility of tracking stolen items, and we may hear more in later panels this afternoon about what the future might hold.

To the extent that people are talking about notice to consumers and choice about whether or not to
kill tags, because there might be these applications
that would be of interest to them if they leave the tags
active, I'm wondering if you could sort of think out
loud for me what that kind of notice and choice regime
would look like and what kinds of burdens it might
impose on consumers.

For example, are we going to get privacy
policies where we have to make kill choices every time
we go to the grocery store or the office supply store or
a clothing store on an item-by-item level basis? Can
you give us a sense of how you envision the notice and
choice sorts of protections working?

MS. HUGHES: Well, I can start. You know, we
already have some guidelines in place that really deal
with the technology the way it is today, and basically
that's giving the choice to the consumer and notice on
the products. So, I mentioned before, for example, that
we are putting tags on our cases, you know, just for the
chance that it could actually end up in a consumer's
hands, even though that's not our intent.

I think that that will probably continue to
evolve as we get more education out there, where
consumers start to know that when they see the EPC
symbol that's on a product, just as they would, you
know, "kosher" or "recyclable" materials, that they
would want to know what that is, but that's a huge, massive education campaign to be able to get to that point.

As far as choices, I think as the technology starts to develop, you know, there will be all different kinds of things that could be possible. It might be, you know, a vision that people see for the future, is that all your products are tagged, they will be in a smart cart, and you can just kind of walk out, you know, because it will know what your purchases are, and you put your loyalty card in there, your credit card, you know, you don't even need to talk to anybody or see anybody.

That's really far off, but it might be that there would be some sign that would come up, you know, to the consumer as they're putting in their loyalty card, or let's say even through like a "you-scan," that says, "Do you want your tags killed or not," or something like that, and then it just automatically does it when it scans the tags, and there is no intervention required at all. I mean, that could be a solution. It's a process as well.

There are also guidelines that may need to be put in place. So, it's not all technology, and it's something that could be self-regulated as well.

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
MS. GIVENS: Yeah, and I brought something with me, I'm so glad you asked this question, because now I can do my show and tell. This is a TrackPhone package, and I am quite certain it has an RFID tag in it. It's right next to the magnetic theft protection device, but I'm pretty sure that's RFID.

What I would do with this, just from a -- I guess one of the things that we do as the Dear Abby of privacy is we also try to quash conspiracy theories when people call us and ask us, is such and such really true? What you could do here is just put a red dotted line around it that says, "EPC tag" or "RFID tag," and if it's something that the individual kept live and wanted to keep for warranty or to attach to their receipt if they needed to return it, they could cut it out, put it in a little mylar sack and store it.

I mean, I think probably I'm a little bit of an unusual consumer in that I'm a consumer advocate by profession. I do keep receipts. I do know about the fact that you don't have to keep things like this or the product registration cards that you get in the packaging to return an item, but there are some things that I think that the industry could do to reduce the conspiracy theory problems, and that would be clear labeling, and also, never, ever, ever embed an RFID tag

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
in clothing, in shoes, in one's eyeglasses, in anything that is worn or carried by the individual, and I agree with Lee Tien, that includes driver's licenses and passports. But I think just clear labeling, enabling individuals to destroy them if they want to, keep them if they want to, of course, kill them if they want to.

The other thing is I think individuals should be able to have their own readers or go someplace where they can read what they have on their person or what they think they have.

I think those are the extent of my comments. I think there's a lot of things, though, that industry can do to allay suspicions and fears, and labeling is a big one.

MR. LIVINGSTON: Okay, this is for John and Sandy. Was the RFID consumer study, the Capgemini study, peer reviewed and published in a reputable research journal? Can other researchers get a copy of the methodology used so they can attempt to replicate it? I ask because previous studies conducted by the Auto-ID Center, including one done in conjunction with Procter & Gamble, found that consumers were very opposed to RFID on both privacy and health grounds.

MR. PARKINSON: So, it was not a peer-reviewed study, was not published in any kind of formal journal,
reputable or not, but it is published by us, and the
protocol was actually done by a third party to a design
that we co-developed, and the protocol is published.

So, what questions we asked, what was directed,
what was undirected and so on is available, and we are
happy to open all that up so anybody else can replicate
it on a different population. For economic reasons, we
are a business, not a research organization, so for
economic reasons, we limited the panel size to a
statistically valid profile. So, we did take account of
gender, income, geography and education to the extent
you can in a small sample survey.

It was just over a thousand respondents when the
survey was cut off. The results have statistically
meaningful inferences, but if you did the study a
thousand times, you would get a distribution of results
that would deviate somewhat from the percentages that
we've produced, not necessarily in our view by very
much.

MS. HUGHES: And I can talk about the research
that was done by the Auto-ID Center, and it wasn't done
by P&G, but we let them use our services since we are
pretty good at doing market research by consumers, the
number of tools that we have available, and one of the
outcomes from that study as we did find out how
consumers perceived the technology is to implement from
the Auto-ID Center the Independent Advisory Council
that's been led by Elliot Maxwell, who you will hear
from later today. So, that was a direct action that
came from research that was done by the Auto-ID Center
and a number of the members of Auto-ID Center where we
saw that there were concerns from the consumer sector,
and we did something about it.

        MS. FINN: Thank you.

Another question from the audience, has the
regulation of RFID already begun? Is this workshop a
sign that it's begun? And at the state level, seven
RFID bills were introduced this year in five states. Is
this a good thing or a bad thing?

I am going to answer part of this question, is
this workshop a sign that regulation has begun. The
answer is no. From the FTC's perception, we often have
these workshops, and they are not a precursor to
regulation.

But as to the other aspects of state regulation,
maybe Bill and/or Deirdre would like to speak to that.

        MR. MacLEOD: Well, I think it is probably
premature to say that RFID regulation has begun, but it
would also be misleading for the reasons I've stated
before, and that is RFID is a very well-defined problem

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
in the consumer protection space, the consumer protection agencies recognize, and they will address it if RFID becomes in any way misused to the detriment of consumers.

So, once again, we don't have to have an RFID bill or an RFID regulation by either a state or the Federal Trade Commission, but I can guarantee you -- and I can do this because I no longer work at the FTC and I don't have to qualify my promises -- if someone uses RFID to start disseminating personally identifiable information contrary to their privacy policies, they're going to have the FTC all over them. They're going to have the states and they're going to have plaintiffs' lawyers as well. In that respect, RFID is indeed regulated, and it's the kind of regulation that we should welcome.

MS. MULLIGAN: You know, certainly there are state efforts to regulate RFID, primarily, kind of in the consumer marketplace. I think that probably what you got from the opening panel was that the use of RFID spans lots of different markets and has lots of different implications regarding privacy, and you know, the kind of legislation or the kind of self-regulatory guidance that you might develop in the Procter & Gamble, you know, EPCglobal commercial space would be I would
imagine quite different than what you might see developed for the invisible man, and so my guess is that, you know, we're going to continue to see, as we always do, legislation that, you know, is kind of brought about by the latest article in the newspaper.

My hope would be that while the FTC may not be looking to regulate, this is at least part of the beginning of a dialogue about how to institute best practices, how to develop public policy. Whether or not that public policy has a heavy regulatory component I think is a separate question.

MR. LIVINGSTON: Okay, I have two questions here which are related I think, so I'll ask them both, and I guess Sandy and Mallory and anyone else, of course.

We've heard that EPC/RFID tags will cost 20 cents to $20 and a reader is $500 to $1,000. For the billions of cases of products moving through the supply chain, who is paying these costs, i.e., a $10 item with a 25 cent tag is now going to cost $10.25? How is the consumer saving? That's one approach to this same question.

The second one is, I've heard that Procter & Gamble spends $3 billion in the supply chain every year getting products to the customer and can potentially save $1 billion by using RFID. Will consumers ever see
a reduction in prices from this kind of corporate savings?

MS. HUGHES: Well, overall, the whole supply chain is involved in the savings. You mentioned the savings, but you don't talk about the cost that goes along with it. So, we're still working on a business case that would come about, but the end result is that, yes, we're doing it for consumers. I mean, that's the reason why we're there, as I mentioned before, we have the product they want on the shelf when they want it at the right price, and that all goes together.

So, it's not just price-oriented itself, but it's the whole shenanigans, the whole thing that you see on the shelf, the first moment of truth, are we meeting what the consumer wants or not?

MR. DUNCAN: And Ted, I guess because you were asking two questions, one was really an apple and the other was an orange. The first one was really talking about I think the expensive tags that are used at the pallet level, and there the savings are spread across the entire pallet, and it's much more significant than the same tags used at the item level.

As to whether the savings is passed onto consumers, the honest answer is people can't expect to see a dollar-to-dollar pass on of savings, because a
dollar saved, you won't see a dollar more, because retailers don't compete that way. The way we compete is by taking whatever it is they do best and trying to deliver that as an incremental value to consumers.

For example, Neiman Marcus and Saks don't compete by offering $25 off on the merchandise they sell. They compete by having the kind of sales force in the store that consumers who shop there want to see there. That's a very different model than, say, Wal-Mart, which is trying to shave every cent off. So, yes, there will be savings, but they will appear in a different form.

MS. HUGHES: And just to qualify some of the numbers there, for us, at case and pallet even, you know, we've said that it needs to be done at 5 cents a case. So, we are way far away from that, and if you consider any further down to item level, as I mentioned before, you know, some of the prices of our products, there need to be, you know, some really major savings to offset the costs so that we can even, you know, provide the same price, or we just won't do it for consumers. As I mentioned, it's the whole delivery to consumers there.

MS. FINN: Another question is, have any of you determined whether database collection of RFID data
linked to an identified individual violates European privacy law, and how do you get meaningful consent to linkages like that with such low levels of consumer awareness? It didn't specify who should answer, but if anyone wants to volunteer...

MR. PARKINSON: Okay, so I work for a European company, so this is something we worry about every day. The fact of linkage does not violate European law. It's what you do with the linked data afterwards that puts you at threat, and there are gray areas here that the legislation was not designed to deal with, particularly the movement of goods which carry information with them across national boundaries, which in some interpretations is just by itself illegal without the consent of the carrier, which could be an individual.

When the original privacy legislation was written, nobody had thought of that. So, we expect to see some evolution of practice and policy leading to evolution of legislation in Europe. It gets even more complex when you cross territoriality, because it's just as easy for me next week when I'm going to be in Paris to pick something up which could be tagged and legal in Europe, fly back to the United States, and have it tagged and illegal. So, this is not just a North American problem. The supply chain is global.

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
Seventeen percent of everything that you buy is made in China these days, and it's on a rising trend. So, we have to start thinking about what are we going to do to harmonize our point of view about acceptable practice on a global scale, and consumers are going to be everywhere, and they can buy goods no matter how marked.

You might, for instance, want to think about perfectly valid market legislation which requires you to learn Chinese in order to know what was marked. Those are the types of issues that you start to look at when you look at it on a global scale.

MS. MULLIGAN: I haven't looked specifically at, you know, how the European Union Data Protection Directive would map onto RFID, but I do think, you know, when you talk about pushing data out to the end points, we've focused before on kind of distributed computing, and you know, there are some very difficult questions. So, for example, to the extent that -- when you take the library as an example, in order for somebody to access information at the library, they have to come with a subpoena, but now they could, in fact, reconstruct it, because there is some information on the book that allows them to kind of easily assemble that. Would it be in violation of the state law?
You know, I don't know what it would look like, but you have kind of the question about how does this impact with kind of the general public policy framework that we've put out there, and these kinds of, you know, cheap, inexpensive broadcast technologies that potentially store information that you can connect to other databases or that is a pointer to a database, and you add in some stuff that hasn't been talked about yet today, the EPC object name server and the EPC discovery service that are about kind of tracking a particular good as it moves out of all these distributed points, whether it's with readers, or enabling you to find a point or two database that gives you more information, I think there's lots of questions about how our general privacy framework, which really was developed in the time where there were very specific data collectors that had the information and nobody else did, it was centralized, they had kind of responsibilities, and these kinds of systems really start to pull at that kind of framework.

MS. HUGHES: And let me just pick up on what John was saying about the EU. For us, and I mentioned this before, being a global company, we source globally, so product made in one country we will source to another. It's really important for us to have global
standards, and this is for everything, you know, from
the technical aspect as well as privacy, and you know,
the European Union is kind of, you know, still trying to
decide how they feel about RFID, and we're working with
them as well.

So, you know, as much as we appreciate forums
here, we're doing the same thing in Europe, and we will
be doing the same thing in other regions as well, so we
come out with some common solutions, but within Europe,
for example, some countries can't agree on whether it
falls under the current EU Directive or whether it
doesn't, et cetera. So, there's a lot of work that
needs to be done there on all fronts.

MR. LIVINGSTON: Okay, here's one for Beth.
We've heard today that there are consumer RFID
applications -- drugs, meat and tires come to mind --
which can save lives but require an item-level tag. In
many cases the consumer benefit is enhanced if tags
remain after sale. Does the position statement on the
use of RFID on consumer products which your organization
has co-sponsored and which calls for a voluntary
moratorium on the item-level tagging of consumer items
apply to these categories?

MS. GIVENS: Well, the position statement, which
you could read at privacyrights.org and also

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
spychips.org and some other Web sites, has a couple of attachments to it. One of the attachments is a discussion of RFID applications that would be considered beneficial and would not be problematic to the individuals and organizations that signed onto that. But I want to return to something I said earlier. I think some benefits can come from not necessarily EPC tagging, where there's a unique identifier for each can of Coke, but as I mentioned, there's certain types of tagging that could be generic, for example, that identifies a toxic. It could just say, this is lead, this is nickel cadmium, when you take it to the landfill.

So, I think that when we're looking at the privacy impacts and the solutions for mitigating some privacy threats, I think we could look at different ways of implementing RFID that don't necessarily uniquely identify that item that is then held by that individual. So, I think there are lots of kind of creative things that can be done that mitigate the privacy impacts or the potential privacy impacts.

MS. FINN: I have another question, and Dan, maybe you can answer this or anybody else who thinks that they -- maybe it's a little more technical.

Right now, in terms of the possible solutions
that might help consumers, we have heard a lot about
kill functions. Does killing RFID tags have to be all
or nothing? To the extent that there's a potential for
beneficial uses of tags remaining on, is there a way to
have tags not be so promiscuous, to allow consumers to
leave them on but only to be read by authorized readers?

MR. WHITE: There have been several things
talked about in the industry, in fact, we talked about
within our company about a couple ways to do it. One
mechanism kind of goes along with what Beth is saying,
is just killing the serial number and leaving the
product code and manufacturer code live. We talked
about ways of just tying into a transaction, maybe
rewriting the code, and it's no longer individual items.

There's also some IP that we have put in about
disabling the tag for range and maybe kind of shooting
it in the leg so you can't read it more than an inch
away or you actually have to have it up against
something to read it. So, there are multiple technical
possibilities as we look at this in the future that are
beyond just killing it.

Killing may be what we want to do right now,
just because we want to work through a lot of the other
issues before we really address it, but there are a lot
of different ways to solve the problem, where someone
couldn't read it if they didn't want to. You can encrypt the thing where you have to have a certain reader in order to actually read the tag, a lot of different things that the consumer might be able to use in the future.

MR. DUNCAN: I think we have to be really careful when we talk so promiscuously about the idea of killing technology, because the unintended consequences of that run deeply as well. We've talked a lot about the imagined consequences from the privacy perspective, but in terms of trying to develop new markets for these products, you want the products to have a life so that those markets can develop.

For example, I mean, one of the not very far outside ideas, we demonstrated this at the NRF show this year, was the smart refrigerator and the idea that if there is sufficient demand for it, there can be products within the refrigerator that can read the products there, the other merchandise, and let you know whether or not the milk is out of date, whether or not you're low on certain normal staples, and have a possibility of having the refrigerator re-order for you, yet no one's going to go to the trouble to develop that kind of technology if a significant proportion of the public is going to say, we ought to kill this without having a
good reason to kill it. So, I think we have to keep in
balance the benefits and the costs.

MR. PARKINSON: And you have to remember that
the architecture for deployment we're working with today
means that the tags are dumb. What you get off the tag
is a bit stream. It doesn't mean anything. It's just a
number, and unless you know how to decode the first
eight bits of the stream, you don't even know what kind
of number it is. Without being able to hit a reference
server, an object name server, to find out what that
stream means, all you've got is a bunch of numbers.

The controls -- we could encrypt those so that
they don't even mean directly what they mean when you
individually manage to decrypt them. Control of the
object name servers and how you get to the intelligence
that tells you what that stream means should be the
primary place to start applying policy, because that's
an easier, at least for now, form of control.

Long term, we can build scenarios that will put
all that data eventually into the public space, because
with enough cheap computing and cheap storage, you can
reverse-engineer the content of the object name servers
into public versions, just like you can now with CDs and
movies. But you can't defend this with technology, and
I don't think any of the technologists looking at this
believe that technology is the answer to all of this, but right now, it's part of an answer, given a clear policy on appropriate use.

MR. LIVINGSTON: Okay, here's one for Sandy and Mallory.

Have P&G and/or retailers uncovered implications of RFID for consumers that it did not expect or predict during its pilots? If so, what were they, and were they beneficial or detrimental?

MS. HUGHES: Well, we haven't found anything that we didn't know already, just confirmation of the point that the more education that consumers are given about the technology, then the more understanding they have and more acceptable they are to it, which just outlines the work ahead of us as far as the education.

MR. DUNCAN: And I would just mention one point that was demonstrated by the Capgemini/NRF study, that consumers tend in the abstract to undervalue some of the potential new uses, more than a lot of people think.

MR. LIVINGSTON: Here's kind of a fun one that I don't know much about, but it's for Beth and Deirdre.

Does the current Coca-Cola promotion using the SIM chip locator tags through the GPS system violate privacy rights? If so, how?

I don't know how anyone can answer that.
MS. GIVENS: I think I am going to show that I am not a typical consumer. I honestly haven't been following that campaign, so I really don't have a very good answer on that one. It would be interesting if someone on the panel is following that campaign and knows what in the world he just said.

MR. PARKINSON: Okay, so a SIM chip is a subscriber identification module chip inside a cell phone, which in GFN and certain other types of cell phones tells you who it belongs to. It tells you who it belongs to by linking it back to a telephone company referential database.

New generation phones also contain GPS technology, which allows the mobile 911 service to figure out within about a hundred feet, in ideal conditions, a hundred meters on average, where that phone is. So, Coca-Cola thought it would be cool to give you the opportunity, if you opt in, for it to tell you where the nearest case of Coke is if you want to buy one holding your phone.

MS. GIVENS: It sounds as though it has an opt-in, and in order to participate, you would have to be fully informed as to what you're up to. It sounds to me as though it would comport with the privacy guidelines that I'm comfortable with, but again, you
would have to know a little bit, and like I just evidenced, knowing that your phone has a SIM chip in it, I certainly know about GPS, but I think a lot of things go together to make up kind of informed consent in a situation.

MS. MULLIGAN: Location information is one of the areas that we have kind of more protective rules, and without looking at the actual information that's being given to consumers, I would hate to give you a legal opinion.

MR. LIVINGSTON: I won't hold you to it. Okay, here's one for Dan and probably others would like to comment on this.

A number of speakers have suggested that consumers should be given the ultimate choice of whether they want the products they buy to have RFID tags. How do we educate them so they can make an informed choice? Is that a reasonable expectation?

MR. WHITE: I have had to do a lot of educating in the last year. We have had 100-plus retailers come through, and I think the concepts, if you keep them simple and you just explain, you know, at a fairly low level what's going on, I think they can make sense, because there's enough other technology that's similar. We've mentioned cell phones, for example, could be
considered an RFID type of situation.

I do think that no matter how much you try and provide information, there are some people that probably won't read it, and you have to take into that account, and you have to do your best to try and be up front and honest about them, and I think to provide that in a way that people can get access to it, I think that's about all you can do, because you can't force people to do something they don't want to do.

MS. HUGHES: Again, you know, as I mentioned before, the education, you know, whatever was done to really recognize symbols before and what they've come to mean is something that's going to, you know, take a long time to do through all different types of media and different types of forum, but until then, I mean, what you've seen before and what Simon told you about what was in the video, is just to get in the face, for example, of consumers as they are buying a product.

HP printers at Wal-Mart, there were these shelf tear-off tags that consumers could take with them, and the labels that I mentioned that were on cases, and you are welcome to come by and read one of these. It's got questions and answers on what is electronic product code, et cetera, and on the back, and the value to them.

The ones that are on the cases say, for example, to

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
improve product availability for consumers, packaging contains electronic product code. Upon purchase, the EPC tag can be discarded, and it gives the Web site address of EPCglobal, Inc.

So, I think there is going to be some overt things that we need to do until we get to the point where it's common knowledge.

MR. LIVINGSTON: I have a two-part question. Is point of sale the best place to do that, and the second is sort of a rhetorical question, I guess, would it have been better for the retailers and packaged goods companies that have done the various trials over the past couple years to have made more of an effort to communicate in that way?

MR. WHITE: My understanding from the retailer side and dealing with retailers, point of sale is not the place to do anything. You want to get them out. So --

MR. LIVINGSTON: I guess I meant more the shelf than the point of sale itself.

MR. WHITE: Okay, now the shelf, where they are actually shopping, where they may be trying to make a decision, that may be the place. We've also had people talk about a consumer service desk to provide further information, have people there to maybe answer

For The Record, Inc.  
Waldorf, Maryland  
(301) 870-8025
questions, they might want to understand what's going on in the store, and the Web site. So, I think all those areas are applicable, and trying to do it in the store, where it's at, is probably the best place. I don't think you could do it any other place.

MS. GIVENS: If I could add something, I think we can learn from the privacy notices that came out starting in July of 2001 regarding the financial institutions. I think something that should be avoided is what I call happy face technology, with a happy face, and kind of overselling, doing the marketing hype, you know, RFID is a technology that's going to benefit you and make life wonderful and satisfying and oh so convenient.

I think it's better just to keep the messages simple and factual, and I think that consumers -- those who at least pay attention to such things -- mistrust something that's got kind of an aura around it of hype and an oversell.

MR. LIVINGSTON: Okay, we have got time for one or two more. Here are two related questions.

The first one, and this is for John and anyone else who wants to comment on it, can you clarify what actual information is sent out or not sent out by EPC tags and how they are read?
And relatedly, it sounds like there are no more privacy concerns with EPC than with bar codes. Is it different?

MR. PARKINSON: So, there is no such thing technically as an EPC code. There is a set of types of tags, and the type determines what you get when you read it. They range from tags that are active, so they're powered, they transmit and can be picked up by receivers in a very wide area, down to the kinds of tags that will eventually go on consumer goods cartons, which are not powered. They are a chip plus an antenna with a 96-bit code in a format defined by EPC in the chip.

To be read, they have to be within -- their spec says about 20 feet, but the practice commonly is running 10 to 12 feet, although a power reader broadcasts a low power radio frequency field which causes the chip in the tag to pick up just enough energy to send out the bit stream of what it is, which the reader then picks up, and what it picks up is simply the set of codes, and there are fields within the code.

The first field says what kind of code the rest of the fields are. So, you could use the tag format for lots of different things, including proprietary coding schemes if you choose to. So, you can make them exactly identical to bar codes if you want, as the Auto-ID
Center and EPCglobal have done a very good job from a technical perspective in building a lot of flexibility into the scheme that tags and reader combinations use to work.

To figure out what the rest of the bits mean, you have to refer to an object name server that has the lookup tables that said, okay, so field one says 25-26-34, that's Coca-Cola. Field two tells you that it's a 24-pack of 10-ounce cans of Coke. And then you can put some other information in if you want to, which can either be in the three fields on the tag or can simply be pointed to by the object name server, which could point back to the Coke bottler that would tell you when those cans were filled.

So, you have a number of layers of information management in the architecture that you could choose to implement in flexible ways, and at each level, you can choose to put both encryption, no random person can make sense of the bit stream, and security, you have to provide permission to get to the next layer of information.

So, is it different from bar codes? There are a couple of critical differences, the biggest being that it doesn't have to be visible on the item. So, I can put a tag inside the packaging rather than having to put

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
it outside, because bar codes must be visible to be
read, but it doesn't have to have any obvious
orientation to the reader, as long as it's within range,
so that readers can be hidden. They can be made
nonobvious in a way that you can't with a bar code or a
laser scanner.

    MS. MULLIGAN: Well, just out of -- nobody has
ever talked to a bar code, right? I mean, you wave it
over -- you read it at the point of sale, and that's it,
and potentially, you come out, and this thing continues
to talk to other readers without being in any contact
with them, and I think for a consumer, that's a very
different experience potentially.

    MR. PARKINSON: I would argue that it's an
extension of an existing capability, because as long as
a bar code is visible, I can read it from almost a mile
away with a laser scanner. I just have to know where to
point it. So, we have changed the detailed nature of a
problem without changing the problem, from what's the
persistence of the information contained in the item and
how do I get to it without the consumer having to know
about it.

    MS. MULLIGAN: I just learned something. I
didn't know you could read them from a mile away.
That's fascinating.

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
MR. PARKINSON: You could read them from orbit if you...

(Laughter.)

MR. LIVINGSTON: Anyone else on that topic? I think we're just about out of time, so I would like to thank our panelists for a very lively discussion.

(Applause.)

(A brief recess was taken.)

PANEL 4

MS. BROF: Okay, we're ready to start up again. I'm Julie Brof again from the FTC, and I'm happy to introduce this panel, which will be maybe slightly longer presentations and talking about, again, looking ahead, what can we expect, and we have some pretty distinct visions of the future represented by our panelists.

Starting off this panel we'll hear from Chris Boone with IDC, who will address the promises of RFID versus reality, examining deployment in the supply chain, item-level tagging and consequences for consumer privacy.

As a program manager covering the retail, wholesale and CPG manufacturing industries for IDC's Vertical Industry Research Group, Chris is an

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
acknowledged expert in RFID use in the supply chain. He has presented on RFID in many forums, most recently hosting IDC's RFID Update Conference held earlier this month in Boston.

Next we will hear from Katherine Albrecht, the Founder and Director of Consumers Against Supermarket Privacy Invasion and Numbering, or otherwise known as CASPIAN. CASPIAN is a national grass roots consumer group dedicated to cutting supermarket loyalty or frequent shopper cards; CASPIAN's efforts are directed at educating consumers and condemning marketing strategies that invade shoppers' privacy and encouraging privacy-conscious shopping habits.

As many of you if not most of you are aware, Katherine and CASPIAN have been extremely active in raising awareness about the consequences for consumers of RFID use, beyond the supply chain in particular. Katherine holds an Undergraduate Degree in Marketing and is currently a doctoral candidate in education at Harvard University where she is writing her dissertation on consumer education and privacy.

We will conclude this panel with Jim Waldo, who I had an opportunity to see speak at an RFID conference in Seattle last month. So, I can say from personal experience that he is not only knowledgeable but pretty

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
funny, too.

He is an engineer with Sun Microsystems Laboratories where he researches large-scale distributive systems. Like Katherine, he can also be found on the Harvard University Campus, where he is an adjunct faculty member of the computer science department.

Jim will be discussing what the future of RFID will be expected to bring as well as what it will likely not bring. So, let me turn things over to Chris.

MR. BOONE: Thanks, Julie.

Again, my name is Chris Boone, and I'm a program manager with IDC. For those of you unfamiliar with IDC as a company, we are an IT market intelligence and research firm that is actually celebrating our 40th anniversary this year. Our main focus is to work with IT vendors, and then secondarily, we typically work with the financial community to understand market opportunities around hardware, software and IT services, the size of those markets and forecast their growth into the future. So, it gives me great pleasure to be here with you today and present our vision for RFID specifically within the retail supply chain and try to answer the question whether or not this really is the next big thing, as it's currently being touted.
So, just quickly going through the agenda, we will start with a brief discussion on promise versus reality. We won't spend much time about promise, because that's been talked to death I think today. We will spend a little more time on the reality side of that slide.

We will then talk about the RFID ecosystem for the retail supply chain as we see it, again very briefly there, and that is going to build into I think the crux of the presentation, which is our forecast for RFID within the retail supply chain, how we think it's going to be adopted over the next five years, and then a long-term view as well, and then briefly touch on consumer privacy, because that's also going to be the main focus I think for today's panel.

Oh, and by the way, you won't find me on Harvard's Campus, even though I live in Boston, so one of these kids is doing his own thing.

So, the promise, as I mentioned earlier, I think has been talked to death today. There is a lot of promise around RFID. It is the oldest new technology out there in the marketplace. I won't go through this specifically. The one thing that hasn't really been mentioned too much on the promise side which I think should be highlighted is that with RFID, because we will
eliminate the line of sight with how the technology
should work theoretically, we are actually going to be
able to speed up the velocity of goods in the supply
chain literally on a conveyor belt. We will be able to
move goods much faster than we can today with bar codes.
In some tests, it's on the order of ten times as fast
when it actually is optimized. So, that actually is
something we haven't talked too much about today.

But the reality of the technology is that it
still costs too much. We have been tossing around
prices of tags, 20 to 40 cents. We actually think on
average it's a little bit higher today. That 20 to 40
cent number is when you make orders in large volumes
today. So, it still costs too much to deploy this
technology on a broad scale.

Standards are still in flux. There is no one
global standard for tagging goods with RFID and
electronic product code that will work everywhere within
one frequency band. Hopefully by the end of this year,
through EPCglobal, we will see such a global standard
that will take into account other standards, such as
ISO, and work in different regions of the world, but we
are still waiting for governments in certain regions of
the world to determine what they are going to do in
terms of UHF, how much power can be used to read those
tags. So, that's an issue for the global supply chain. There still is a lack of end user knowledge. I think by now the top hundred suppliers for Wal-Mart are pretty well versed in how RFID works, but the remaining members of their supplier community are probably not as well versed. The 34,000 suppliers of the Department of Defense also, who will be coming on board slightly outside of this realm, are still just learning about this technology, and they are all struggling to build a business case around it.

From a technical aspect, there are issues of interference. We have talked about this today. UHF tags don't like metal. Is there metal in a warehouse? Yes. UHF tags don't like water. Is there water in certain consumer products? Well, yeah, Coke -- oh, wait, Coke has also got metal, crap. So, we have issues with interference, from the products and also where the technology is being deployed.

There is an inability to read 100 percent of tagged cases once they're put on a pallet. I think it was mentioned in one of the earlier presentations that we could do this. It's still more theoretical. When you actually put the cases on the pallet, you typically can't read the products on the inside because the products are causing interference. Remember what we

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
just said about Coke? So, the true visibility is not
necessarily a reality.

The work-around that's been going around right
now is that you take all the electronic product codes
from all the cases and you assign them to the electronic
product code on the pallet, so when the pallet runs
through, in theory, all those cases just ran through the
portal as well.

Pilots are going on to see how we can figure out
how to make that technology work better, place the tags
better within certain products, use different tag
designs to get around that. One frequency in tag design
does not fit all. Today we've been talking a lot about
UHF, but we have also mentioned high frequency or 13.56.
We are going to see that probably at item-level tagging
in the future.

And there are a number of Wal-Mart suppliers who
want to be good Wal-Mart suppliers, so they want to
comply with Wal-Mart's mandates, but they can't figure
out how to make a positive business case beyond
compliance yet, even at that pallet and case level.
They know that's the first step, but they don't know how
to move much further beyond that. So, building
long-term business cases is still the challenge.

If we take a look at the ecosystem today, just
quickly on this slide, most of what we have been talking about today is the bottom part of this slide, it's the tags and readers and technology, and every company that is going to deploy this within their architecture is going to have that layer, but that layer then is basically an enabling technology as we've talked about. It supplies data up to the enterprise, application and system infrastructure layer of each company, and then each company has got their own business processes, and these are specific to an industry as well as to an individual company.

So, what's important for these companies to ask is, not necessarily how am I going to comply with the Wal-Mart mandate, but what am I going to do if I have access to realtime supply chain data at a more granular level than I do today, and how is that going to make me a better business? So, instead of compliance, we have got to start building business cases at the top level.

We also need to be able to share this data somehow. We think it is going to be through some sort of partner exchange or portal. I don't believe there will be this ubiquitous network that's talked about because I don't think there's a business case for it today. Wal-Mart doesn't want its competitors to read tags that are from Wal-Mart stores. Wal-Mart probably

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
also doesn't want its suppliers to read information about other suppliers. They want to control that information for competitive reasons. So, we think these are going to be somewhat private exchanges. Wal-Mart will probably leverage retail links to do this and other retailers will do something similar as well.

Okay, let's move into the adoption. This slide has a lot of data points. I put them up there because I know it will be available on the Web site, so I am not going to go through all of them here, just touch on some of the key points for our forecast, which is on the next slide.

We talked a lot about the mandates that came out last year that are driving this marketplace forward. We think that the new global standard from EPC will become finalized probably in the fall, but we won't see tags for that available until the end of 2004, and that means there will be a lot of testing that still has to go on around those tags. We think the tag's average cost is about 50 cents, because not everyone is buying tags in high volumes.

By January 2005, we think there will be partial compliance with the Wal-Mart mandate. What does that mean? We think probably all top hundred suppliers, give or take a few depending on what product lines they sell,
will be tagging pallets and cases that go to Wal-Mart. Where are they going? They're going to three distribution centers out of a total of 108 distribution centers Wal-Mart has in the U.S., and they probably won't be tagging all cases and pallets that go to those distribution centers. They're only going to be tagging those that make the most sense from a business case perspective: fast-moving goods, high-margin goods.

Procter & Gamble, I don't know, we could ask, is probably not going to tag every single product that goes to its distribution centers. They probably can't afford to do it yet today. They want to make sure the technology works first. So, that's what I mean by partial compliance by January 2005.

By 2006, we think we are going to see more retailers deploying RFID -- Target, Albertson's made announcements, we haven't heard from them since. We think there will be other retailers that will be doing similar work. We may not hear official announcements, but we think that's going to happen, and these deployments are going to start to pick up next year and continue to broaden in 2006.

Walmart has already said actually they are going to go from three distribution centers to six distribution centers by June of next year, and then to

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
13 distribution centers total by October of next year, and ramp up from 150 store back rooms to 600 store back rooms by the end of 2005. So, we're still only going to be at 20 percent of all Wal-Mart's retail stores and about 13 percent of their distribution centers at the end of 2005.

Moving into 2007, we think we're going to be at close to 100 percent compliance for Wal-Mart's mandate amongst all suppliers. Again, we don't know exactly how far Wal-Mart will be expanded at that point in time, but we think suppliers will have gotten to a point where they are moving in lockstep with Wal-Mart, and actually by 2008, here in the U.S., we think that these pallet and case-level deployments are actually going to be expanded to the point where we won't be deploying more readers necessarily, but what we will continue to do beyond that is spend on tags and maintenance.

So, actually, we think the market is already going to start to flatten at that point in time. We will reach we think that elusive 5 cent number. That's actually just a factor of our model. We weren't trying to get to it, but when we saw how many tags we thought would probably be purchased, that was the number we actually arrived at.

So, what does it look like in terms of spending
over the next five years? We thought the market was approximately $91 and a half million at the end of last year, going to about $1.3 billion in by 2008. You will notice how it's very close to 2007, that leveling off trend happening there. You will also see that we have some fits and bursts in 2005 and 2007, and this forecast says that hardware is making up the largest portion of the number. This is different from what some of the other speakers have talked about today.

The reason why we think hardware is going to be so high is that even though tags are going to be cheap, 5 cents at the end, we are going to be buying a lot of tags by 2008. Software and services are a bit small in this forecast, because we've limited our definition very specifically. So, we just kept it to RFID middleware and just services to deploy the technology, nothing more.

And very quickly, because my time is up, we want to show you a long view here. We think that we're going to have a peak around 2008. We think it's going to decline beyond that, as we're trying to figure out how to do item-level tagging in the future, and that won't pick up for quite a number of years off. There are going to be a number of technical and cost challenges that we still won't be able to overcome until well

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
This follows a similar pattern to other "next big thing" technologies. Those of you who followed the PC market in the early eighties may recognize a similar growth pattern, big boon, bust, then a real wave of growth happening well beyond that. We think that's going to be the case here as well.

Then consumer privacy, I am going to leave most of this to I think Katherine's talk here. It is a top concern. State legislation has been introduced, we have already heard in a number of states about a consumer's right to know if the technology has been deployed, and I think the take-away message from this is regardless of legislation, what retailers and suppliers should not do with the technology is just as important as what they can and should do with the technology.

And here's my email address if you need to follow up with me afterwards. Thanks.

MS. ALBRECHT: Thank you, Chris, for that overview of how RFID is coming.

I'm Katherine Albrecht. I'm the Director of CASPIAN. Many of you in this group I'm sure know me as a consumer privacy ally, and others of you perhaps know me as the person who shot down the Benetton trials and gave them some headaches last year, that they engaged in...
some unannounced and secret trials involving consumers and RFID.

I am going to fit about a half an hour worth of slides into about 15 minutes, so I am going to advise anybody sitting in the middle, if you would kind of like to position yourselves so you can see the slides, this is a very slide-centric and image-heavy presentation I am going to be delivering.

For those of you who are not familiar with our work, you can find it -- our primary RFID work is on spychips.com. My background, as Julie mentioned in the introduction, is fighting supermarket loyalty cards and other forms of data collection. You can find that information at nocards.org, and there, of course, is information on our two boycotts, which were Benneton and also Gillette.

I think one of the key things to keep in mind here in understanding and separating out what the privacy issues are revolving around RFID is the difference between essentially three databases, and I've developed this myself as kind of a way to help to untangle some of the privacy concerns versus just looking at supply chain issue-types of questions that have been raised.

The first database is the one that any company
manufacturing something would be looking at on the factory side. When something rolls off an assembly line, as it moves from the assembly line onto a truck, into a warehouse, into a distribution center, that would be the first database. That database really doesn't pose any issues for consumer privacy.

When I say "database," what I mean is that when you put an EPC or an RFID tag into an item when it's manufactured, the only information contained on the cheapest versions of those tags would be the actual EPC number or the unique ID number. That unique ID number in and of itself doesn't really communicate anything in the same way that your social security number doesn't really communicate anything, but when you link it up with databases, that's when you can find out information about where you've been, where you've worked, what credit you've applied for and other information about you. It's similar here. So, the first database we've identified is not really involving any privacy concerns for consumers.

The second one is the database that enables you to know, if I scan an item and I see what the item is, I can look that number up in the ONS system or in whatever EPCglobal makes available to Wal-Mart, for example, to know that what it just ran over its scanner is a bottle.
of Pantene shampoo, for example. If I can scan your briefcase or your wallet or your purse or your pocket and I can get that number back, I can look it up and essentially know what's in your briefcase, your pocket or your purse. There, I think the implications for privacy are quite obvious to consumers.

Let me jump ahead to these slides. This is the first one, database number one, Cherry Chapstik produced on assembly line 12 at 3:15. No one is particularly worried about that from a privacy perspective.

Database number two, I scan your pocket and I discover item blah-blah-blah, 308247, I'm shortening that down to the end. If I look that up in what will be the widely available EPCglobal database, I will be able to determine that that is a Cherry Chapstik, and I would know what's in your pocket. This poses the most obvious privacy concerns for consumers, but to be perfectly honest with you, this is the one I'm least worried about.

The reason I'm least worried about it is because I think it is so incredibly apparent to people that it is problematic to have the person sitting next to you on the bus know what's in your backpack or know what's in your suitcase. So, I think consumers in their own and on their own will object to this, to the creation and
the use of this type of database with these tags or having the tags live, because I don't think there's any way we can control the use of this database.

The third one is the one that I'm concerned about, because it's invisible, and it's far less obvious. This is the database that gets created at the point of sale. So, now when I go into a Wal-Mart and I buy that Cherry Chapstik number 308247 and I pay for it with a credit card, or let's say I walk into an Albertson's or a Safeway and I pay for it with my loyalty card, even if I pay cash, I've identified myself, and that information. Currently, what few people realize, although perhaps in this room many people realize it, is that currently when you pass through a checkout line and you go to the point of sale and you present anything at all that identifies you, the information of your identity is linked in that store's database along with the SKU numbers or the bar code numbers of the items you bought.

So, in other words, most retailers, most major national and international retailers, are maintaining databases right now on consumer purchases linked up with the bar code numbers of what they buy. That in and of itself is quite problematic.

It becomes more problematic when it doesn't

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
just -- and I think the comment was made right before
the break, was that these don't pose any more of a
threat to privacy than bar codes, and in reality, they
pose considerably more threat than a bar code,
because -- well, there's two reasons.

One is I can't read what's in your pocket right
now if it has a bar code on it. You would have to
actually show it to me and hold the bar code up to a
reader within the line of sight. That's simultaneously
one of the downsides and one of the tremendous benefits
of this technology.

The other reason that it's very different from a
bar code is that it's difficult -- I can link a bar code
up with your identity, and in fact, retailers do that,
but essentially, if I have access to that record, all I
would know would be that you bought Cherry Chapstik. I
wouldn't know which one, and the which one becomes quite
important in a way that we will look at here.

This database three that links up the EPC
numbers or the unique ID numbers with consumers is, I
believe, quite likely given the current what we call
retail surveillance environment in place in retail
stores today. The concern here ties in when you have
item-level tagging. I believe this image is from
CheckPoint. It is working on integrating their

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
anti-theft devices with RFID tags with unique numbers
that would beam over a distance, and of course, as you
can see on this image, it would be virtually impossible
for the consumer to know about them.

Combined with ubiquitous readers, which I'm sure
if you read the literature of people selling this
technology, these readers can be embedded virtually
anywhere in the environment, in walls, doorways, floor
tiles and carpeting. Combined with current levels of
retail data capture and abuse, and I'm going to talk
about that more in a moment.

I believe that all of this combined will lead to
widespread surreptitious consumer surveillance. For
those of you who have been following the RFID issue
through 2003, you might recognize this. This is a
picture of the smart shelf from Gillette, which was
tested at Tesco stores in Great Britain and at Wal-Mart
stores here in the United States. We call it the spy
shelf.

Essentially that little device under there was
detecting the presence of the Mach3 razor products, and
when one was picked up, the camera took a close-up
photograph of the shopper's face for anti-shoplifting
purposes.

So, the other thing we're concerned about is the
use of hidden tags. These images actually came from the Auto-ID Center, and again, anyone who's been following this issue will know that last summer we uncovered some unprotected confidential documents on the Auto-ID Center's Web site. Among those documents were slides showing hidden tags. If you see a six-inch tag, it looks like it would be difficult to hide in a product, but the following slide in their presentation shows it sandwiched in cardboard, literally hidden between the layers of paper in the cardboard.

Here's a six-inch tag, this is actually made by Alien, and this has a 17-foot read range according to my own experiments with it, and these were hidden in the tops of Pantene shampoo bottles. For anyone who buys Pantene, which was my brand before I began boycotting Procter & Gamble products, this is the type of lid that flips up, so the consumer would never actually realize that there was a tag inside of there. Again, we don't know where these were sold. We don't know who they were sold to. We have repeatedly asked them for a clarification, and we have not received any.

Another big tag, four and a half inches, and this one was placed between the layers of paper on Purina dog food, again, according to Auto-ID Center slides, and that would go between that greasy inner
layer and that inner paper layer, where you wouldn't
normally be pulling that apart. So, I gather if you
bought that brand of dog food, you wouldn't be looking
there for it.

Getting even worse, these RFID chips are getting
quite small. This is the Hitachi MU chip, which is
unbelievably tiny there. It would be easy to hide this
RFID chip, particularly if the antenna were made of
conductive ink, and that's one of the directions that
the industry is going to, because they're cheaper, to
print the antennas on using conductive ink and simply
stick the little guy onto the conductive ink, which
could actually form part of the package, and the quote
here, with these things, you can literally tag a pack of
chewing gum. They have mixed the conductive ink with
regular packaging ink to create antennas on boxes of
cereal and other disposable packaging. So, literally
your box of Kellogg's Corn Flakes could contain an RFID
tag and be remotely read without your knowledge.

The other thing, tags being left active. This
is a quote from Wired Magazine. Sandy, you -- I believe
it was from the RFID Journal, when Sandy Hughes spoke,
it was reported she said that P&G and other companies
suggested they want to keep RFID tags active after
checkout rather than disabling them with so-called kill
machines. The companies also want to match the unique
codes emitted by RFID tags to shoppers' personal
information.

If you combine all of that with individual
tracking and profiling, what you see up there on the
screen is a blank for a Matrix RFID enabled loyalty
card. I actually encountered one of these cards when I
went in January to tour the Future Store, the Metro
future store in Rheinberg, Germany. That is the store
that the retail industry is touting as the future of
retailing, and if it is, then we are all in deep
trouble, because what I discovered at that store was
that unbeknownst to any of the shoppers -- and by the
way, 22 million Germans carry this pay-back loyalty
card -- unbeknownst to any of those shoppers, they had
hidden an RFID tag in the loyalty cards and distributed
these to customers.

I discovered that in the presence of television
cameras, and it was a huge scandal across Germany. It
was front page news in a number of their newspapers and
was top of the evening news, and they finally were
forced to recall those cards, but that's a great example
of what happens when you have a desire to track
consumers and it's not tempered by the consumers'
ability to know about it.
This slide you see here is from Texas Instruments' Web site, ubiquitous readers. It actually says, "Consumer loyalty mechanism with TI RFID," and it shows a woman walking past an antenna, and as you'll see, her loyalty card is being read right through her purse, and there is really no indication that she is aware of that happening.

This is an image that was up on Alien's Web site for over a year and a half. This comes from Forbes Magazine, but at the top it says, "As the shopper enters the store, scanners identify her clothing by the tag embedded in her pants, shirt and shoes. The store knows where she bought everything she is wearing."

Now, the chances of that are actually unlikely that the store would know where she bought what she was wearing, but the chances that they would know what she was wearing are actually quite likely.

All right, this comes from a company called Copy Tag, and it shows a worker walking into a room, but what you'll notice is hanging off of him are a number of different tags. Now, the idea is that this doorway would be reading those tags. For us as consumers, those tags might be better concealed. They might be in the tags of our clothing or our underwear as Benneton had planned. They might be on our loyalty card in our

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
pocket.

And then this final slide of ubiquitous reading devices actually shows how you can rig carpeting with electro or actually electrical sensors. In this case these are actually little light sensors, so this is a bit of a stretch, but it has been experimentally proven that you can easily embed RFID reader devices into carpeting, hide them under floor tiles and put them in other places. So, the idea of walking around and actually have the environment sense you and what you're wearing is quite disturbing.

Now, NCR, who is here today, is interested in associating purchase data with unique tag numbers. This means actually linking up your name with the tags on you, so I suppose later, when someone who has access to that database reads the tag, they can determine who you are. They include in their 50 ideas for revolutionizing the store through RFID, including the date of purchase, the name of the individuals associated with the product, the date of the sale, the price of the sale and other information, actually having that linked in the database with those tags.

So, as you can imagine, if your shoe is the only item on planet earth that contains unique tag number 308247 and someone reads tag number 308247 and looks it
up in the database, they can determine who you are and where you bought that item. The who you are is the quite worrisome part, because it creates the potential for tracking people all the time.

I actually put this slide up here not realizing that Marty Abrams, who is the subject of the slide, would be in the audience today. He actually talks about CRM, customer relationship management, which is the invisible layer between the retailer and consumer. It's estimated to be between a $10 and $15 billion industry of essentially gathering consumer data and in my opinion manipulating it in order to manipulate consumers. It involves an incredibly complex network of surveillance, and one of the things that Marty explains as the purpose for this surveillance, he says, "Maximization means 'marginal service and high prices designed to drive the unattractive customer somewhere else.' In other words, CRM facilitates customized pricing and customized service based purely on what the data and models tell you about the potential profitability of the customer."

So, the reason they want all of this infrastructure to determine who you are is so they can either -- I believe Marty, as you put it -- treat you with kid gloves or the white glove treatment. I think if you're a shopper they want to cater to you, and to
discourage you from shopping at the store with higher
prices and poor service. So, what this might lead to is
as I walk into the store now with my pay-back loyalty
card in my purse and you see the tag on there and you
say, ah, this isn't just a shopper we should welcome as
any other shopper, this is Katherine Albrecht, and we
don't like Katherine Albrecht, so we are going to offer
her higher prices and poor service.

You can also do the same thing not only with a
customer loyalty card, disturbingly enough, but you can
do the same thing with any product I bought in your
store. So, if I bought a Cherry Chapstick in your store,
you can use that to look up information about me. You
could sell that information to other people so they
could determine what kind of person you think I am, and
anywhere I go where you can read my Cherry Chapstick, by
linking it up with a database, you would know who I am
as soon as I walk in through the doorway.

Procter & Gamble says we can trust retailers
with this information. Procter & Gamble says,
"Retailers selling its goods can be trusted to guard
consumers' privacy even if they decide to match their
personal information with the serial numbers from the
RFID tags." I say the retailers can't be trusted.

This image is an actual promotional image, if

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
you can believe it or not, this guy with the magnifying
glass standing in a grocery cart is from a company
called PathTracker. They actually -- let's see,
"Records the coordinates of a shopper from the time they
enter the store and select their shopping cart until
checkout, becomes a database for each shopper tracked."

In addition, the path data can be tied to the
shopper's actual purchases. They are using a
combination of RFID and GPS technologies in grocery
carts to literally follow people around the store,
identify them at the point of checkout and link all of
this information together, and at this particular image,
it is an image of the exact track that a shopper took
inside of a store.

Now, imagine how much easier this would be if
you had an RFID instead of all this expensive
PathTracker technology, because the RFID will already be
in place on the shelf, so you can simply determine who's
walking past in addition to reading the products on the
shelf. Who's doing this? These are PathTracker's
clients, and as you can see, they are some of the
biggest retailers in the country. This is just a
partial list.

And this slide, I'm almost to the end here, this
would have been an IBM image of a very sophisticated

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
technology that actually showed people walking around,
and it put boxes around them and identified them as
person one, two, three and four, and tracked their
actual movement around the store in real time on a real
video, and they're using the surveillance cameras you
think are there to stop shoplifting for that purpose.

This video does the same thing, but it does it
to cars and people. Once again, RFID is much more
cost-efficient for doing this, especially if it becomes
ubiquitous.

Of course, Michelin is looking at putting it on
tires, meaning that all you have to do is put reader
devices on roads, and then you would know every single
person who drove on that road. There is even a company,
Applied Digital Solutions, that wants to embed these in
people. Already they've began trials to do just that.

Our concern is that ultimately, if you put this
technology into this current environment, which is
already so surveillance-happy when it comes to consumers
and so intent and willing to violate consumer privacy,
that we believe the abuse is inevitable.

These are just a couple of protest images. I
take great exception to the referenced consumer study
that shows that consumers accept this technology.

Hundreds and hundreds of thousands of emails later, I

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
can tell you consumers really don't like this technology, and they will do everything in their power to fight against it. So, I'll just leave you that as a warning.

Real quick, Proctor & Gamble, Wal-Mart, have not exactly been aboveboard with their trials. We have had some problems with Gillette as well, which you can learn about on our Web site. You can see images of the tracking devices. This will all be available in the slide presentation on the FTC's Web site, and we will put it on our spychips Web site as well.

I will leave you with that image. This was the protest in Rheinberg, Germany after consumers discovered that they had had loyalty tags -- RFID tags hidden in their loyalty cards. They actually turned out in quite a bit of snow when the roads were shut down to turn out to the store and protest.

On that note, I'll leave it as a note of caution. I'll also say that we have worked successfully with several retailers and consumer product companies in discussing ways that they can mitigate some of the privacy concerns.

Thank you very much.

MR. WALDO: So, making the standard disclaimers, I am not speaking as a representative of Sun
Microsystems or much of anybody else. I, in fact, bring you greetings from Planet Geek and will talk on it that way. So, first of all, I -- also, as part of this, by the way, I am one of those guys who will receive the 70-some odd percent of the money going into RFID. I do software for distributed systems, and we can talk about what you do with all of that data. It turns out actually RFID tags generate a lot of data, almost all of which is uninteresting, and I'll tell you why later.

But let's start off by being precise, because this is something that almost never happens in discussions of RFID. Lots and lots of things are called RFID, and they have lots of different characteristics, and it's important to understand the distinctions.

RFID tags are, at least in my lexicon, defined as using RF wireless technology, transmitting only a unique identifier, and either using passive or battery power. Now, there are lots of things that do that and a bunch more, so earlier today, we heard somebody say, well, you know, your cell phone uses RF, and it does have a unique ID, so it's an RFID device. No, it's not. If it were just an RFID device, you wouldn't use it. It's a cell phone, right? It does a lot more than just transmitting an unique ID.

RFID tags are not sensors, they are not
actuators, they are not dumb computers. If they were
dumb computers, they would be really dumb. What they
are is identification tags, that's it, and that's what
I'm going to talk about.

Now, even inside of that, there are interesting
distinctions between things like active RFID that you
use for automatic payment of tolls, physical access
control, some of them are being used to slap inventory
indicators on containers on container ships, things like
that. These things tend to have batteries. That's why
they're active. They can actually generate RF
themselves. They don't have to be yelled at before they
respond.

But they also have some other properties. They
are large, they have big antennas, and they are
expensive, and that expense is not going to go down a
whole lot, because the expense is not in the chips. The
chips are cheap, right? Getting something that
generates a 96-bit ID is not hard. The hard part is the
antenna and the battery. And while chips, thank God,
are still operating under Moore's Law, antennas and
batteries are not.

Right now your battery on your laptop has about
the same data density as a stick of dynamite that size
or about same energy density. You don't want it to have
any more energy density than that. This is why you shouldn't burn those things, because they act even more like dynamite then. So, those are the active ones, but they're expensive. They are like, you know, 40 or 100 bucks a pop. You put them on expensive things like containers, right, or to make sure that, you know, you can put them in things where people do weird stuff like pay money by them, right, then people are willing to spend the money.

Then there are the passive RFID chips, right, the ones we've mostly been talking about today, which can be little, bitty tiny things; however, the antennas have to be fairly large, because they not only have to generate out this stuff, but they have to get all of their energy by shooting radio frequency at them, and the wonderful thing for us who are worried about privacy -- and I am, although I am one of the bad guys -- is that radio frequency stuff obeys an inverse square law, right?

Some of you took physics, I know you did, even though this is the highest tie to T-shirt ratio audience I have spoken to in years, but some of you took physics, so you know what inverse square laws are. That means that if you want to read something at 20 feet that you have been able to read at 10 feet, you need not twice as
much energy, but the square of the energy, and squares
go up really fast for those of you who didn't take
physics, right? For those of you who are the lawyers,
that's really big, okay? So, those are the passive
ones, and that means that you can't read them from very
far away.

Now, everybody's talking about these passive
things can be read at ten meters. Well, they can be
read at ten meters in Texas Instruments' labs under the
best of conditions, but not in the factory and certainly
not on the street. On the street, you're lucky if
you're going to get a meter or two out of them.

I was talking to the guy that you are going to
be hearing from Marks & Spencer, he is saying, no, no,
you know, you have got to get up real close, because it
all depends on how many of the tags you're reading,
because you're basically shouting at them and they're
shouting back, right? One of the things about RFID is
that they are the computing equivalent of
three-year-olds.

All they do is tell you, "I'm here, I'm here,
I'm here, I'm here, I'm here." They don't tell you much
else, and in fact, it's even worse than that. It's not
"I'm." It's, "A long number is here." So, they are
like three-year-old computers, and that's not very
helpful if you are getting all bunches of them, because then they have things that have differential backoffs.

So, if you want to get 100 percent read, you have got to be pretty close with fairly sophisticated equipment, and you have to make sure inconvenient things like metal and water and other stuff that gets in the way isn't there. So, those are -- now, you have all heard about that.

What I am going to urge you today is don't confuse the categories. Don't cross the beams, all right? There are RFID tags that can be read from a long way away, but when you think of that, think really expensive, not going to be useful very much. There are the ones that can be really cheap. They get read really close by. Don't fall into the trap of saying, oh, it's RFID, they can be really cheap and read from a long way away, which is what a lot of people are worried about. They can't.

Now, even the passive ones can be read in some sense without you knowing about it, but remember, you need an antenna about the size of a plate, you need to be within about three feet, and to get any further back, you have to start generating the square of the energy so that if they're reading from very far away, you're not only going to get your stuff read, you're going to get a
tan, and so you'll notice these things, okay?

Now, what's it going to be like tomorrow? Oh, man, I have got to go really fast. What's it going to be like tomorrow? Passive tags will expand to pharmaceutical tracking, government supply chain, military inventory, all that stuff we have been talking about, and that's about it. Active tags, military identification, right, those guys are willing to pay extra money, right -- it's all ours, but they'll pay it -- and more pay as you go.

The technology challenges for the foreseeable future are not putting more information in these things. The first challenge is cost reduction, the damned things cost too much. And the next three or four iterations of Moore's Law on this is going to be cost reduction. And then the next problem is they still cost too much, because the antennas cost too much. And beyond that, there's a real problem in getting the chip-antenna bonding to work right, because as you make these chips smaller and smaller and you try to attach them to the antenna, it gets harder and harder. So, you know what happens when it's hard to attach these things? They cost too much. So, those are going to be the first three things.

Beyond the foreseeable future, what they're
going to be working on are things like transmission
reliability, reader reliability and the administration
of readers. I don't know how many of you have ever
administered a network of computers, but every time you
add four or five computers in, and each one of these
readers is a computer, every time you add three or four,
the cost of administration goes up by a lot more than
three or four, right? It gets a lot more.

So, this vision of ubiquitous interconnected
readers, while it's a nice vision, will cost more than
anybody can afford to do it. None of these companies
that are doing RFID want ubiquitous readers. They want
them in a couple of places. In fact, most of the ones
I've talked to don't even want them out on the shelves,
because out on the shelves -- which by the way is where
they get their 50 terabytes of data a day -- it's too
expensive. It's 500 bucks a shelf, and in Wal-Mart,
there's a lot of shelves. They don't want to do that.

RFID tags, remember, are really bad sensors.

Now, there are people doing interesting work in trying
to use them as sensors and inferring all sorts of stuff
from them, kind of invisible man things that are going
on, and those are interesting, but they are only good at
one thing, which is they can tell you that they are
there. They can tell you the number that's there, and

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
they're good at being cheap, although they are not as good as being cheap as they should be.

Using them as sensors requires that you be really clever and come up with all these inferences, and by the way, whenever we're clever and we're coming up with inferences, we're generally wrong, and if by noticing second or third order effects, and you end up being wrong a lot with second order effects and being wrong even more with third order effects, and the thing is, we know other ways of building sensor networks.

They're called sensors, right?

You want to find out if Grandma turned on the faucet? Well, put a sensor in the faucet. Don't put it an RFID tag to find out if she came close. Put a sensor in the faucet to find out what the water flow was. Hello? Is this that hard? You know, I mean, we're geeks, and so we like to do that kind of thing, but let's get real here.

So, most people, I will claim, are not going to notice RFID tags, because there's not going to be much of anything to notice. There may be attempts at automated checkouts where the RFID tag is going to have a reader in the shopping cart. By the way, you are going to be damned sure that you are going to know about that, because it's going to be large. There may be

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
product information kiosks or shoplifting protection systems.

By the way, when I tried the shoplifting protection systems, they don't work very well, because it's so easy to block these things. There are not going to be many of those, because the cost is too high, the benefit is minimal, and as we are seeing today, the politics is ugly. Not you, the politics.

Now, here is my favorite RFID paranoia. This was an ad on the internet for an RFID sniper rifle. It supposedly has a range of a thousand meters, can insert an RFID tag into somebody, they won't feel anything more than a mosquito bite, and you will be able to track them by satellite.

Now, this appeared on the internet, and they got orders for it. Get a grip, folks, all right? They not only don't understand the RFID technology, they don't understand the physics of shooting things a long way, right? If you can shoot something a thousand meters, then if it hits you at ten meters, it's going to blow a hole in you that you don't want to think about, but this is an example of where people are in their thinking.

Now, in some sense, I find this very complimentary. They think that technologists like me, we can do anything. Ooh-ha-ha-ha-ha. We can't. Get

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
over it. We can't. And even if we could, it doesn't mean that we would.

So, RFID is important. The technology has lots of promise for things like greater economic efficiencies, superior control over goods, convenience in certain applications, mostly in the supply chain, but it's not going to change our world, be noticeable by everyone or change the way we compute.

Now, this doesn't mean, by the way -- and this is for my friends that are privacy advocates, and I do have some -- this doesn't mean that there aren't real privacy concerns going on, but the privacy concerns shouldn't be around RFID, because every time you hear privacy concerns about RFID, it's RFID tags allow you to access the database, right? That's what the phrase is always. The problem is accessing the database.

Now, we know how to secure databases. We have been doing that for a long time, and the question is, what should our policy be on databases, not what should our policy be on RFID tags. It's the information that gets gathered.

And in fact, I was pointing out at the break that were I, in fact, a mad scientist instead of a merely pissed off one, that I would think it would be a great thing to get people all stirred up about RFID.
privacy so that they would be worried about that, and I
could go off and invade the real privacy on the
databases myself. Ooh-ha-ha-ha-ha. That's what we
should worry about, not the RFID stuff.

With that, I thank you.

MS. BROF: And thank you, too, and I think we're
really out of time, but I think we got a pretty complete
picture of some of the concerns, what we shouldn't be
concerned about, and maybe a challenge to the next panel
when we're talking about some of the technological fixes
that are proposed that -- I mean, one observation is
that the full title of this workshop should not be
"Radio Frequency Identification" but "and Database
Access," and I think everyone sort of agrees on that as
being a key, core concern.

So, with that, I give you the next panel, and
they'll be available for questions afterwards, I'm sure.

(Applause.)

(Pause in the proceedings.)

PANEL 5

MS. THORLEIFSON: Good afternoon. I'm Tracy
Thorleifson. I work with Julie Brof in the Regional
Office in Seattle, and I'm glad to see most of you still
here. I hope this panel can follow up on some of the
previous panel's presentations and also in coming up
with some solutions or recommended solutions.

With me as a co-moderator is Elliot Maxwell. Mr. Maxwell is a corporate strategist and attorney who consults and writes on the intersection of business technology and public policy in telecommunications and electronic commerce.

If he wants to elaborate on that more, I'll let him, but he is an expert in this area, and I'm delighted to be co-moderator with him, and with that, I'll turn it over to you.

MR. MAXWELL: In the interest of full disclosure, I'm also the last three years or so the Chair of the International Public Policy Advisory Council for MIT at the Auto-ID Center on this technology, and I also do that for EPCglobal.

Let me just sort of make a couple of remarks before we start off. This technology is really interesting in lots of ways, and one of the ways that it's interesting is it's a traditional infrastructure technology, and what does that mean?

One thing it means is that anybody who says that they really know how it's going to be used and all of its ramifications is absolutely wrong, because what we'll find is that there's lots of things that will happen with this as the infrastructure develops that

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
nobody ever expected.

Think about the internet and whether we could, in fact, have predicted all of the things that happened with that. We couldn't have. So, even on the positive side or the negative side, we don't know yet, but we know that it's infrastructure.

It also has some very interesting applications in terms of the economics. Imagine building a phone system, right? If you build a phone system and said that the first user had to pay for the phone system, how many phone systems do you think would be built? Zero, because the real value comes when the phone system extends to lots and lots of people, when you connect lots and lots of people. That's all of what network effects were about.

So, the economics of this means that it has to sort of roll out, and yet the burden of paying for it comes with the first users, and so that means it may not go as fast as people have suggested. In fact, it's very likely that it follows another set of rules, and that is that we are constantly underestimating the difficulty of implementing a technology, constantly underestimating the time a technology takes to get implemented, constantly overestimating how quickly these things will happen, because we can describe what we think will
happen, but we forget about the difficulties, and
constantly underestimating the long-term impact of
infrastructural technology.

So, probably when we talk about these things, we say there's a Wal-Mart mandate, and the Wal-Mart mandate is for all of its largest suppliers to be putting tags on the materials that they ship to Wal-Mart, and yet we also know that it's only going to take a very small piece of the Wal-Mart chain of commerce in the first several years. It's not as if like dragon's teeth this stuff appears magically all over the country, all over the world.

So, we have in some ways some time to think about, as this technology plays out, what to do about it, and we have some alternatives to think about how to do it right, and this is one effort today, among others, to think about how to do it right.

A second interesting thing about this technology is that for one of the first times, the interests of corporations in protecting their competitive information is lined up with the interests of consumers in protecting information about themselves.

Now, think about this. As people mentioned before, Wal-Mart doesn't particularly want Target to know what its relationship is with its suppliers, and

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
Gillette doesn't want Target to know what its relationship is with Wal-Mart, and all along this chain, the companies are saying I have got incredibly valuable information I want to protect.

Similarly, consumers are saying in many instances, we want to be sure that you control the information that you get, who has access to it, what they do to it. So, we need to be spending a lot of time thinking about this question of access to databases, but we are, in fact, lucky that those two things are in line, because what it will mean is that there are going to be people thinking from both the corporate side and the privacy side about how to deal with this question of access.

The third thing that we should be thinking about is that there are usually a number of different ways to deal with public policy issues, and it's usually not binary. It's usually not you do one or the other. It usually is a combination of a number of things.

So, you think about consumer education, you think about what the technology can do, you think about what the individual companies can do, and you also think about regulation and legislation. Each one of these may play some role in the development of this technology, and it's not clear right now what should be assigned to

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
which, but what we need to be thinking about are what's the appropriate way of responding to the issues that people have raised so far today.

People have started to talk a little bit about the state legislation, and the FTC has I know thought a lot about this, invited some people at the state level to come, and they weren't able to come, but it's one of the ways that people are responding to the issues.

Let me just make one point about that, because if you think about this technology, people around the world are going to have access to this technology, and when the people who are driving the technology think about it, they think about global solutions. So, to the extent that we think about solutions to these issues, we should think about them in a global context, and in that context, it's not as if we're kind of writing on a blank slate.

When someone asked before, are you going to regulate RFID, there are already rules around the world about some of the issues that have been raised today, whether it's the EU Privacy Directive, and a number of European countries have already said that data collected through these means are subject to the Directive, but it also means spectrum rules, it means health exposure rules for radio frequency, it means individual consumer
protection laws, whether at the state level or at the federal level or at other national levels.

So, it's not as if there aren't kind of already are things in place to address some of these questions. So, as we hope during this panel we'll be thinking about what already exists, what kinds of solutions exist in consumer education, in industry practices, in regulation and technology, to see what fits best at a time when the technology is still evolving and when the goal is to have something that, in fact, operates globally.

So, with that in mind, let me turn it back to Tracy as to the order of the speakers, and we'll start right away.

MS. THORLEIFSON: Well, I am going to introduce each speaker as they get up to speak, and to begin with, I am very delighted to introduce Mr. James Stafford from Marks & Spencer, who definitely wins the prize for coming the longest way, because he came from England. This panel's title is "Meeting the Challenges: Best Practices and Principles," and we bring you Mr. Stafford because he has met the challenge at his store, Marks & Spencer, and he's here to talk about that.

His title, our favorite title of all the panelists, is Head of RFID. So, Mr. Stafford from Marks & Spencer, Head of RFID.
MR. STAFFORD: All right, thank you very much indeed, and you can be clear from that whose head is on the block if things don't work out very well. It's great to be here all the way from England, and it's about the time now, about five hours ahead, and I would be settling down with a cup of cocoa, be settling down to go to bed.

I have spent my whole career involved with innovation and new technology, and a risky business it certainly is. I think that it does seem to me that in a retail context, we really have to be very careful of anything that involves new technology, because on the whole, people are cautious about things which are new.

So, I think if you want to deploy new technology, I think you first of all really have to think about engaging with your customers and re-assuring them that the benefits of this new technology outweigh any potential perceived risk of that technology, and I use the word "engage" with care, because "engage" doesn't mean talking to them. "Engage" also means listening to them as well, listening to what they have to say. So, here's what we've been doing using this new RFID technology.

That just says here I am in Washington.

Okay, just a little bit about Marks & Spencer,

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
which you can read on the Web site in the notes. The key things here, established in 1884, we're over a hundred years old. I have been there for a great deal of the time, feels like it. We have got three really or four separate businesses, clothing, foods, homeware and financial services. We have 10 million customers a week. We have 300 stores in the UK and turn over around about $14 billion, and we are the UK clothing market leader. And we have got stores, large stores, departmental stores, High Street stores, stores which specialize in food, and stores which specialize just in homeware.

And we're using RFID to drive efficiency in our supply chain, and here, where it does require a little bit of concentration here at this time of the evening, we have got two separate business deployments, because we're using this technology in two different parts of our business. We're using it in foods, and we're using it in clothing, and not surprisingly, because they're different businesses, the business case that drives us to use this technology is different in foods and in clothing, and again, it shouldn't be too surprising that the iteration of that technology is different, because there is not just one RFID technology, as people have said, there are many different types, and we use them
differently in foods than in clothing.

Now, I'm not going to say very much about foods, because -- only really just to kind of boast the technical people here who are really using this thing, that we have already deployed 3 and a half million RFID tags on our returnable food trays, plus some other deployments as well within foods, and these are trays which are filled up with foods by the food supplier, and they are sent through to our stores through a depot and then returned empty back to the food supplier in the first place.

The white square on the right-hand side of that tray, underneath that white square is buried the RFID tag, and at the actual supplier, we are writing information to that tag in place of the previous paper label. So, here is a deployment where an RFID tag is being used to replace traditional paper or bar coded labels, and basically every trip, we write to the tray what the contents of the tray is, it's a tray of potatoes, and it's a certain bag size, and it's got a certain potato, got a certain sell-by date, it's probably a particular variety of potatoes, other information is written to the tray, and when the tray comes back empty after the next trip, the next set of props is written to it.

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
The advantage of using RFID tags over traditional bar codes is entirely because we can read the RFID tags much more quickly than we can read traditional bar codes. The business case for using RFID tags is entirely around the speed of read, and it's a pretty easy business case to make, because this is a returnable tray situation. These trays last seven to ten years, they make two and a half trips a week, and so you can see the amortization of the tag cost is really spread over something like 1000 to 1500 trips over the life of the tray. So, it's really very easy to make this work for us.

But I don't really think, as Katherine said earlier, because this is not some, you know, in the consumer-facing end of the business, that it really actually involves many privacy concerns.

When we came to the trials of clothing, we have done our clothing trials on menswear, and this is about item-level tagging. This is about the item-level stuff that you've heard about isn't going to happen for many, many years to come. Well, welcome to the future. Here in London, we are five hours ahead in time and ten years ahead in technology, it appears to be, from what I've heard today, and in this case, this is a read-only implementation of tagging of clothing. We did a trial...
last autumn to test the technology in our store to make
sure it worked, and now we've gone on to a larger trial
this spring in six stores to prove the business case for
using this technology.

Why should we be bothered to use this
technology, item-level? Well, basically we want to
improve the stock availability for our customers, and we
believe we can make the supply chain more accurate by
using this technology, and of course, it's retail
heaven, we have all heard about it, right goods, right
place, right time, and that's what we are trying to
drive for, but it is also consumer heaven, we believe,
because it means that your shopping trips to a store are
not wasted, because we'll have, at the very least, the
size of the item that you're looking for.

We've also tried to really talk about it just as
another stock control system and said that really, being
a migration of stock control systems from krull pins
through Kimball tags and bar codes, and now to the RFID
technology, which we are calling the intelligent label.

These are our intelligent labels which we're
using, which we're hanging on the garments. They are
quite large, they are very visible, and if anybody wants
one afterwards, I have got a few here, I will give them
to you. If you're an RFID vendor, it will cost you a

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
hundred dollars. It's all about small volumes, you know, high prices. But we also try very hard to communicate both to our staff and to our customers about what this technology is all about, and we made a video which we made early this year to try and get the message over.

(Videotape played for the workshop participants.)

MR. STAFFORD: That's the -- oh, we don't want to do it again, do we? Now we're completely losing it. Let's just -- I just can't get rid of it. Somebody help me. Oh, click out there, that's a good idea. There we are, excellent, sorry.

Anyway, the video has been useful. A number of people commented it would have been even better if it had some decent actors, but we did have a budget.

Just a few words about this to really emphasize some points made by the video. Again, as we have all talked about, the information on the tag is just a unique number plate. We are not writing any information at all in this deployment to the tags. So, on our central database, we are kind of matching up the tag number and the information about the garment, about the size, style and color.

Even if you get the tags and can read them,
eventually you could hack into our database, again, all
you'd find out was that there was a certain garment of a
certain style and a certain color. There is no customer
information ever recorded on these tags, and
furthermore, we're not even reading the tags at the till
points, so there can never be any confusion about what
we're actually doing.

Here's a tag, as we've shown you, on a garment.
It's fairly obtrusive. It's a bit too large. You want
it to be visible, but it sticks up behind people's necks
when they are trying the garments on, but at least it
does the job.

Here is the mobile scanner built into a Marks &
Spencer shopping trolley. This is Mark II. Mark I had
smaller wheels, and it is now on bigger wheels, and we
have a Mark III in development, which I can't show you a
picture of, but don't hold your breath, because the
current nickname for it is called Lunar Lander. But
this is the reality about what you need to do to deploy
the technology.

Most importantly, we've provided in our stores
and on display in the current trial is a leaflet for the
customers, which basically has two sides, a first side
that tries to explain a bit about the technology. The
second side, most importantly, talks about our

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
commitment to our customers, and it talks about our
responsible use of the technology, and we're committing
ourselves to say they will be clearly identified, these
intelligent labels.

They do not contain a battery. They are passive. Customers do not need to keep the intelligent labels to return or exchange items. We have a very generous refund policy at Marks & Spencer. You can buy anything from any of our stores at any time and you can bring it back at any time and get a full refund, even without a receipt. So, we do take back a lot of items from our customers, although we are lucky they keep some of them, but basically, whether you've got the RFID labels or not, it doesn't affect our refund policy.

We will not link any garment information on the intelligent label with customer details, and we will not scan intelligent labels at the till, and you may, as a customer, of course, throw away the intelligent label after purchase.

Furthermore, we will also remove the intelligent labels at the till point if you request it. All the staff are briefed to do that, and that is what we're doing now, and I think that's the end of my presentation.

Thank you.

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
MS. THORLEIFSON: Thank you.

Our next presenter is Elizabeth Board, and she is with the EPC Public Policy Action Committee and has done a number of wonderful things in communications and public affairs, which if you want to read about, check the bios.

MS. BOARD: Thank you, good afternoon.

We've been listening to a lot today since my colleague spoke at 8:30 this morning, Sue Hutchinson. She talked about the technology behind EPCglobal. I'm going to talk a little bit about the organization itself, not the technology. I'll also talk about our public policy guidelines that address privacy issues, and I'll encourage all of us to continue the dialogue that's been started here today.

First of all, what is EPCglobal? It's a joint venture of the Uniform Code Council and EAN International. We're new. We were just formed in November of 2003. We're charged with taking the electronic product code from its development at MIT to the global marketplace, and our mission is simply to create global standards for the EPCglobal Network, or as you've heard many times today, the next generation bar code.

UCC and EAN International are the perfect
parents to have for this venture. They have 30 years of experience developing and managing business-to-business standards. Examples include, of course, UPC or bar code standards and electronic data interchange standards for information flow. They are a global organization representing more than 100 countries, and the bar code standards are used by more than 1 million members, and this translates into 10 billion bar codes scanned every day worldwide.

Our vision is efficient global commerce for the ultimate benefit of the consumer. And I'm proud to say that EPCglobal has now over 200 members. That's not a million, but it's only been since November.

Our business is based on some important principles and beliefs. We're a not-for-profit organization. We're neutral. That means we represent manufacturers, retailers and solution providers. We are standards-driven. Our standards process is open and inclusive. We're serving all companies, from large multinationals to small business, and in every business sector, every industry sector. And of course, we have a global perspective.

We offer -- actually, I am going to skip over these slides on today and tomorrow, because you've heard a lot about what EPC offers today and what it could
possibly open tomorrow. I just want to say one thing about where we are today.

If you look at the history of the bar code, at this time in its development, it was drowning in urban myths. In fact, many of the original urban myths involved the bar code. If there was a museum on the mall for urban myths, the bar code would have an entire floor.

In 1975, I was producing a talk show in Washington, D.C., a radio talk show, and whenever the phones would be dead on a holiday weekend or something, I would call up my roommates and say, call in about the bar code, and in five minutes, the phones would be lit, and the debate would go on.

But now, they're everywhere, and no one gives them a second thought, and why is that? It's because retailers never did any of the things the urban myths said they were going to do, and the reason is because it's not in the retailer's best interests to do anything that would make the customer feel uncomfortable.

That's why one of the first things EPCglobal did when it was formed last fall was take over the privacy guidelines that had been developed at MIT. These were developed with input from consumers and privacy experts, and they're managed at EPCglobal by a public policy.

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
steering committee.

    This part of EPCglobal is very important. In fact, you can see on our org chart that privacy is as important as anything we do. It's right there on the same level with our technology steering committee and our business steering committee. This is the business that we're in, and privacy is absolutely a part of it.

    Public policy guidelines have four critical elements: Consumer notice, consumer choice, consumer education, and of course, our members follow all rules recording all legislation, regulations regarding record use, retention and security. Our subscribers agree to adopt these guidelines, and they're being used today in the consumer test phase.

    Simon showed you some of the ways that Wal-Mart used consumer notice in their test recently. On the slide now is the tag that was actually put on the printer box, as you saw that, and Sandy showed you the actual shelf talker, but they did more than that, and that's why I wanted to bring it up.

    They also had a press conference at Wal-Mart. They invited cameras into the store. They did as much as could possibly be done to let people in the local community know that something different was going on.

    It's important to understand about our
guidelines, because they will evolve over time as the technology evolves. These guidelines are for right now, while we're in the testing phase. We're going to need to do things with these guidelines, and that's what the public policy committee is charged with. The guidelines are part of the classic technology launch; develop, launch, learn, refine and improve over time. We will continue to participate in public dialogue and listen to consumers and all of you as we responsibly and ethically deploy EPC technology.

So, in conclusion, I've just made four key points here today. We're a neutral, nonprofit organization driving efficiency in the global supply chain. Our members follow public policy guidelines for responsible use. EPC is in the early stage of development, and urban myths can stifle innovation. And finally, I hope we continue the public dialogue, and I'd like to thank the FTC for this opportunity today.

Thank you.

MS. THORLEIFSON: Thank you.

Our next panelist is Cedric Laurant, who is Policy Counsel with EPIC, the Electronic Privacy Information Center, where he's concentrated on a number of privacy issues, including profiling air travelers, video surveillance and government electronic
surveillance. He's also supervising production of the

MR. LAURANT: Thank you very much. Actually, I
would like to thank the Federal Trade Commission for
inviting the Electronic Privacy Information Center to be
a participant to this panel.

What I am generally going to talk about is
probably a little bit boring. It's the guidelines, the
privacy principles that should guide RFID users and
retailers in the way they implement RFID tagging on
individual consumer products.

I think the Federal Trade Commission has a very
important role to play to protect consumers' interests,
and in that regard, we came out with a set of guidelines
establishing rights and duties for consumers and RFID
users that you can find on the table outside, that some
of you may have already picked up, and that's available
online on our Web site at epic.org.

I am going to refer to a few instruments,
international instruments and guidelines that have been
released recently that show that there are many privacy
experts and many legislative bodies that have taken a
strong interest in how RFID tags raise very strong
privacy concerns for the consumers and that show very
clearly that RFID tagging should be regulated or there

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
should be guidelines that prevent the businesses from intruding into consumers' privacy.

The first guidelines refer to the Data Protection Privacy Commissioners. It's a resolution that the Data Protection Privacy Commissioners came out with in November last year, and those guidelines say very explicitly that RFID design, implementation and use must be based on basic principles of data protection and privacy law, and they basically say that any RFID user should first consider alternatives which achieve the same goal without collecting personal information or profiling customers.

They also say that data must be collected in an open and transparent way, that the data may only be used for the specific purpose for which they would first collect it and only be retained for as long as is necessary to achieve or carry out this purpose; that whenever RFID tags are in the possession of individuals, these customers should have the possibility to delete the data and to disable or destroy the tags.

Another very important reference is the 1980 Organization For Economic and Corporation Development Guidelines and Principles, as well as the American Principles of Fair Information Practices. These guidelines establish eight privacy principles.
The first one is the collection and mutation principle, which requires limits to the collection of personal information and the obtaining of any data by lawful and fair means with the knowledge or consent of the subject, the data collection principles, that stipulates that personal data should be relevant for the purposes for which they are to be used, and they should be accurate, complete and up to date.

The personal specification principles establish that the purposes for which personal data are collected should be specified not later than at the time of data collection, and the subsequent use should be limited to fulfill those purposes.

There's also a use limitation principle, security safeguard principle and openness principle, and this one is very important. It states that there should be a general policy of openness about developing practices and policies with respect to personal data, which means as far as RFID implementation is concerned that there should not be any secret databases. There should be no tag reading in secret. The label should be clearly displayed and easily understood by consumers.

There is also an individual participation principle, which states that consumers, customers who purchase RFID tags, should have the right to ascertain
or confirm whether an RFID user has data relating to him or her and to challenge the data, to be able to amend or correct that data.

There are also accountability principles that state that there must be, as applied to the RFID industry, there must be entities in both industry and government to whom individuals can complain when these provisions have been violated.

Several civil liberties groups released a position, a policy position on RFID last November 2003 in which they enumerated practices that should absolutely be prohibited. Merchants, they said, should be prohibited from forcing customers into accepting live or dormant RFID tags in the produce they buy. There should be no prohibition on the individuals to detect tags and readers and disable the tags on items in their possession. Human tracking, they said, is inappropriate. RFID should never be employed in a fashion to eliminate or reduce anonymity.

So, the guidelines EPIC came up with incorporate those fair information practice principles and the principles that were enumerated in the civil liberties group's statement.

I'm going to go over them very quickly, but what's important, what I would like to stress about

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
those guidelines is that the first part addresses the
duties of private enterprises that use technology in a
way that's analogous to bar codes. A second point that
addresses the duties of private enterprises who go a
step further and use the RFID technology in a way
analogous to loyalty cards, where personal information
stored on the tags potentially contain a profile of the
customers, and finally, a part three that states the
rights of consumers who are exposed to RFID technology.

So, in this part one, what's important is the
fact that RFID users should give notice to an individual
of the presence of an RFID tag. Labeling should be
reasonably conspicuous to the individual, and you should
state at a minimum that the product, in fact, bears an
RFID tag, that the tag can transmit unique
identification information to an independent reader both
before and after the purchase and should also contain
basic technical characteristics of the RFID technology.
RFID users should also not track the movement of
individuals on the premises or outside the premises.

The second part establishes the duties that an
RFID user using RFID system should follow when those
RFID systems gather personal data about an RFID subject.
I don't have time to go over them, but you can find
these guidelines outside on the table and online on the
And just briefly, to explain the state of legislation outside of the United States, which may have an impact on how personal data being processed in the United States, the major one being the EU Data Protection Directive and the EU Directive on privacy and communications, which contrary to what Sandy Hughes said previously, is very clear about how information processed by RFID tags should be regulated. There's no doubt about this. Those two EU directives clearly apply to information that's processed by tags.

There are also Japanese and Italian guidelines that recently came out. So, what we would like the Federal Trade Commission to do is to take a look at those guidelines and try to push the companies to adopt them, to push companies to post privacy policies that embody a set of guidelines that provides consumers with the possibility to actually enforce them, and if there is any abuse related to the data, their data, the processing of that data by RFID tags, the FTC should ensure that consumers can actually obtain compensation for this abuse.

Thank you very much.

MS. THORLEIFSON: Thank you. And just a reminder to everybody, I know it's late in the day, but
if you have burning questions or suggestions, to write
them down and send them up.

Our next panelist is Paula Bruening, who is the
Staff Counsel for the Center For Democracy and
Technology, and she specializes in privacy and free
expression issues. She is going to bring us some more
thoughts on best practices.

MS. BRUENING: Thank you.

Today's panels I think -- well, first of all, I
should tell people who CDT is. I give these talks a
lot, and I assume people know, but the Center For
Democracy and Technology is an independent advocacy
organization, we're nonprofit, and we advocate for free
expression, user empowerment and privacy on the
internet, and as Tracy said, a lot of my portfolio with
CDT is privacy, and I have been working in the area of
privacy for about ten years now, and I think today we've
heard a lot about the potential of RFID, and there is a
lot of consensus that there is a lot of good that can
come from this technology.

I think there's also a lot of agreement that the
technology does raise privacy concerns, and whether or
not we agree on how one would characterize those
concerns, I think there is an understanding that if
consumers and users don't trust this technology, if they
don't trust it as being used appropriately, that the
information is being collected and used responsibly with
respect to privacy, they aren't going to accept the
technology and the many good things that can come from
it.

So, I would say that any decision about
addressing privacy -- and there is clearly a drive to do
so -- must be based on sound analysis, on the input of
all stakeholders, on reliable information, and on a
clear understanding about the technology, both its
potentials and its implications and risks, but already,
we're seeing a lot of movement toward establishing some
kind of principles, guidelines, best practices for
privacy and this particular technology.

We have heard about industry efforts through
EPCglobal and their standard-setting process; we've
heard now about EPIC's principles; and legislatures are
now looking very closely at this now that consumers'
concerns are being raised about privacy. I think what
lurks under all of these efforts is the concern about
possibly institutionalizing solutions to privacy that
have unintended and unforeseen consequences that are in
the end going to stifle either the proliferation of the
technology for the good uses that can come of it or
institutionalized mistakes about how we address privacy

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
and in ways that don't foresee the possible things that
could come of the information collection and the
reactions of users to privacy concerns that it raises.

So, how do we go about addressing this? I'm
going to talk about two things briefly. First, I'm
going to talk a little bit about technology assessment,
and as a matter of full disclosure, I will say that I am
a graduate of the Congressional Office of Technology
Assessment that you have heard a lot about today. I
worked there for five years, and it was a very good
experience. It is an organization that was not without
its critics, as many of those criticisms were well
placed, and I'll comment on a couple of those as I talk
about technology assessment, but I think there's a lot
of good that can come from it, and I would just like to
raise a couple of points on that.

Technology assessment, an assessment of RFID
that draws out an understanding of the technology, of
how it works, its potential to serve users, and the
vision of the future for the technology, how it might
proliferate and develop, and the risks that it raises,
could provide the analytical underpinnings that would
really drive very sound solutions, the best possible
solutions to address privacy.

Such an assessment would benefit from the input

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
of a wide range of stakeholders, experts, technologists, who could really bring to bear some of the best thinking about this issue. As we've heard today, a lot of these efforts are already ongoing. We have heard that things are going on out at Berkeley. There are industry surveys that have gone on, industry outreach, different kinds of efforts in terms of developing guidelines, learning more about the technology and its ramifications, and so I think there are a lot of pieces of this work that are already ongoing and that what's needed is really a centralized point where all of this could be brought together and where some of that neutral analysis could take place and be brought to bear. I think there was a comment in an earlier panel about, well, we don't really need neutral analysis, that we will let the market figure all of this out, and I think that it's really important to understand what that neutral analysis means.

First of all, if you do technology assessment well, you aren't going to come out with solutions. The point of technology is not to drive to the fastest solution that's going to make a certain segment of stakeholders happy. What infuriates many people about it is that you don't come out with any kind of answer. You come out with road maps, you come out with

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
possibilities, and you come out with what's the
consequence if you act in certain ways on the basis of
what we know about a technology.

I think that the other point that I would make
is that if you do it fairly, technology assessment
generally makes everybody a little bit angry and
everybody a little bit happy. I think I really
thickened my skin working at OTA, but inevitably,
whatever we published got heavy criticism and a lot of
praise at the same time, and they often came from the
same people, and I think that that's an important thing
to remember, whatever side of the debate that you're
sitting on, is that whatever you come out with at the
end of this process, we'll all have learned a lot more,
but we may not all be happy with all of the outcomes of
what we find.

The second point that I wanted to talk about,
since time is limited, is best practices. I'm really
excited to hear about all of the work that's going on
creating guidelines, creating some of these high-level
principles, and I think what's really important going
forward is to build on that effort and to start to bring
those 30,000-foot efforts down closer to where the
technology is being used and down to more practical
applications.

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
I'll just point out one example. We've talked a lot about how it's really, really important that consumers get good notice about what this technology is, how it works, what its benefits are and how they can control the information collection around RFID, and we've talked about consumer education, and I would say that we've had enough experience at this point in the area of providing notice to consumers that we know that in different kinds of environments with different kinds of technologies, this exercise can be really, really challenging, and I think that this is a place where we're going to have to do some very creative thinking about how you provide notice to consumers about an invisible technology that provides very passive kinds of data collection, and conveying to consumers in a meaningful and effective way what's happening is going to be a big challenge, and I think you could take that similar analysis when you start talking about things like providing choice and providing accountability.

To make this happen requires all stakeholders sitting around a table and really rolling up their sleeves and doing some very hard thinking about how those very important principles that have been discussed here today are applied in practice. I think that it can be an effort that is labor-intensive, but if we get to

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
work on it quickly, we can come up with at least a first
iteration of something that will work, that we can take
to the marketplace and implement quickly, and as
Elizabeth said, continue to refine, continue to think
about this, and continue to figure out what's going to
be best for us moving forward.

To arrive at these best practices really
requires a concerted effort of all stakeholders and
interested parties, but I think that if we do the hard
work now, we can come up with something that is going to
serve both consumers and businesses and I think
importantly is going to inform further decision-making
about policies about privacy around RFID for the future.

Thank you.

MS. THORLEIFSON:  Thank you, Paula.

Our next panelist is Rob Atkinson.  Mr. Atkinson
is Vice President of the Progressive Policy Institute
and Director of PPI's Technology and New Economy Project
and the author of many other things, but he's here to
talk to us about meeting the challenge in best
practices.

MR. ATKINSON:  Okay, thank you.  I want to thank
the FTC for holding this panel, because I think it's an
important issue.

I have to admit right away, just so you know

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
where I'm coming from, I am an RFID advocate and user. I have my smart card, so if anybody wants to know where I went on the Metro recently, just log into their database. I have my key card, if you want to break into PPI, just scan that. I also have my Mobil SpeedPass to tell you where I've been recently. And not only that, but I have not one but two grocery store loyalty cards, and unfortunately, they don't have RFID in them, so I don't think you can track them.

I want to make four points today. The first point is, I often wonder whether we would even be having this kind of conversation about a really important innovative technology that's going to improve our economy and give consumers choices if it weren't for what I would say are some privacy advocates who are trying to make this out as a major crisis in our lives, and let me just give you a few examples of that.

Before I do that, actually, I think, you know, given how big the benefits are to consumers, given how big the benefits are in terms of productivity, access to quality items and stock, as our Marks & Spencer colleague pointed out, the only way consumers are going to be convinced that somehow they should avoid this useful and innovative, cost-saving technology is to somehow raise the specter of all sorts of terrible

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
things that are going to happen.

Let me just give you a few examples. These are not, for example, from the aluminum foil hat group. These are actually legitimate privacy groups have said these things. Cedric said on his Web site, "Chips integrated into commonplace products such as floor tiles, shelf paper, cabinets, appliances, exercise equipment and grocery and package products would allow even our most intimate activities to be monitored."

All right, I have to tell you, I don't really use my Exercycle in my house, and I often times eat Hostess Twinkies at night, so now you know.

The position statement on the use of RFID on consumer products issued by CASPIAN warns, "When a consumer purchases a product with an EPC-compliant RFID tag, information about the consumer could be added to the database automatically. Additional information could be logged in the file as the consumer goes about her business." Entered Atlanta courthouse, 12:32, at the Mobil gas station at 2:14. So, I guess Wal-Mart will know when I go to buy Mobil gas.

UNIDENTIFIED SPEAKER: Is this constructive at this time of day, castigating people?

MR. ATKINSON: They also go on to warn about kill tags. They say, "Stores would only pretend to kill
a tag when they would make it dormant and later reactivate." So, obviously we shouldn't even pursue kill tags, because stores will lie to us about the kill tag. Knowing that, the government will probably pass a law -- given the Congress, no, they're highly likely to pass a law, to quote, "prevent stores from killing them," and thereby create, "a surveillance society." I know that the Kerry Administration, if it comes about, and certainly the Bush Administration, that's top on their priority list.

Third, Barry Steinhart, Director of Technology program at ACLU, wrote an article in CIO Magazine where he warned that -- basically he was trying to give the male opposition to RFID, he warned, "Imagine strolling around a city one evening and you happen upon a sex shop and pause for a moment to snicker at the curious items in the window. You continue on your way. Unbeknownst to you, the store customer ID system has detected an RF signal emitted by a computer chip in one of your credit cards and recorded your identity. A few weeks later, you're surprised to find in the mail a lurid solicitation from the store mentioning your visit. You've got some explaining to do." Well, I know that one of the major things sex stores do is provide personally identifiable information (PII) on their
customers so they can get them to come back.

The last one is one that Jim Waldo mentioned about the RFID rifle on the Web site. You can laugh at that, but John Gilmore, who's a board member of EFF, Electronic Freedom Foundation, he scoffed at the rifle idea, but he did say this, he said, "People with RFID chips in their clothing, books, bags or bodies could be targeted by smart projectiles that will zero in on that particular tag." This is something we will probably use to get Osama Bin-Laden, we will get him to wear some Benneton clothing.

He also goes on to state, "Imagine being able to bury an explosive in a roadway that would only go off when a particular car drove over it. You could bury these bombs months in advance on any major or minor roadway. You could change the targeting whenever you'd like. You can give a whole list of cars that would explode." I think it would be a little hard to dig up Interstate 95 and put an RFID tag, reader in there, and pour the concrete that night, get it all nice and smooth before the next day, but you know, who knows?

So, in other words, look, what this debate is really about is let's scare the American public, let's scare regulators, let's scare legislators, because this is an awful technology. The reality is, most of that's
technologically impossible, most of it's practically impossible. The Wal-Mart database is not linked up to the Mobil database, so Wal-Mart doesn't know when I go to Mobil. Mobil knows, but I'm okay with that.

Even if technically and practically feasible, which they're not, none of these scenarios will ever happen. Companies, the last thing they want to do is share that information. And the really good thing about this is any egregious practices that companies will do, such as surreptitious reading and other things like that, the really good thing about all these privacy groups -- and it's things that I've given them credit for in the past and will give them credit for in the future -- is they're out there every day eating, breathing, and sleeping this stuff. So, any time somebody violates what are considered as reasonable things, they are going to be out on their Web pages, be on the front page of The Washington Post.

The second point they make is that these technologies will link product purchases to PII, and I really think this is a red herring. Every time I use a credit card, I link product purchases to PII. We've been doing it for 30 years. Most Americans have a credit card. Most Americans are pretty happy with that. If they're not happy with it, they can pay in cash.

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
Third, I think most Americans really don't care about this. I think they see there's no real problem. There are no real harms with bar codes. There are no real harms with credit cards. They use the stuff, and they use it for a pretty simple reason, because it provides them with real benefits in their daily lives.

But that's not good enough, so what privacy advocates want to do is basically make the millions of Americans who are happy with this technology to pay extra money, because if we delay RFID or if we add costs by making the chips so complex to serve all these privacy functions, the cost is going to go up and we are going to significantly reduce the benefits.

Finally, I think in terms of what should public policy do, I think right now, public policy should certainly not consider legislation. I think the main thing we need to be looking at is is the industry likely to proceed along the lines of providing notice, choice when that's feasible, and I think they are, and until proven otherwise, I don't think there's a role for government to basically step in and do anything.

I do think, though, that there are two roles the government has in this area. One is to be an advocate for the technology. One is to say, this is an important technology that's going to help boost American
productivity and make our lives better, so that we can all understand it. The second thing is to work closely with groups like EPCglobal, to make sure that they are doing things like making sure that there are privacy notices and that there is no surreptitious tracking. I completely agree with people that say that surreptitious tracking is bad. If you are going to have a reader, it ought to be out in the open.

If it turns out that surreptitious and rogue tracking is possible, which is a highly debatable point, we can pass laws against that, just like we've passed laws against using cell phone cameras in bathrooms. Did we outlaw cell phone cameras? No, absolutely not.

So, in closing, I would just close by saying I think it's way too early to even consider any type of legislation. This is a technology that's going to have significant benefits for Americans, and we ought to just let it evolve.

Thank you.

MS. THORLEIFSON: Thank you.

Our final panelist, who is going to address some of the ways that the technology is evolving, is Dr. Ari Juels, who is a principal research scientist at RSA Laboratories, where he oversees the various data security projects of the Applied Research Program.
DR. JUELS: Okay, thank you, Tracy.

It's probably fitting that I'm the last speaker of the day, because I would like to contradict most of what was said over the course of the day now.

There has been a polarization among panelists into two camps, into the privacy advocates who view live RFID tags as an absolutely pernicious state of affairs if placed in the hands of consumers, and then industry advocates who pooh-pooh the privacy concerns that the advocates have brought forth.

One question that was posed by the audience to the previous panelists was whether it was possible to have live tags in the hands of consumers and to achieve privacy at the same time. In other words, can we strike a balance between privacy and utility? And I'd like to suggest that the answer is quite possibly yes and would like to give you a glimpse of a technical vision for how to achieve this. I think that we need some complementary legislation, but as a technologist, I am going to talk about this primarily from the technology side and talk about a possible way of achieving this balance.

As a computer scientist and a data security specialist in particular, I view RFID in the following

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
terms: RFID means that we will have a world with billions of ant-sized computers, tiny computers. This is, in effect, a new type of computing infrastructure. We already have a great deal of difficulty securing the existing computing infrastructure, so we have to pose the question naturally: what are the implications for privacy and security when we introduce all of these new little computers into the world?

This is complicated by the fact that these are highly constrained devices from the computational point of view. They carry very little functionality, and in particular, they're unable to perform many of the data security functions that we're accustomed to employing in securing existing computer networks and computing devices. For instance, they can't perform encryption, and in fact, even if they could, encryption wouldn't solve most of our problems, as I'll discuss in the next slide.

As we've discussed over the course of the day, they are subject to clandestine scanning and mobile and personal. These are particular complications here, and computer security is already fairly hard in general.

On the other hand, we've already managed to secure a world with a broad array of computing devices, everything from mainframes to PDAs, and what we've seen
is that with good tools and foresight, we can at least
achieve adequate computer security, and I think that we
can achieve adequate security and privacy with respect
to RFID.

A key thing to observe here is that in places
where we didn't plan well in advance, we're paying the
price now with regard to viruses, for instance, and
general hacking attacks, denial of service, trojan
horses. We didn't think in advance about these security
problems, and they've become extremely problematic and
costly now. So, it's incumbent upon technologists to
try to address future concerns even before the
technology really gets off the ground.

Let's cast our minds forward to, say, the year
2015 or whenever it may be when individual RFID items
are, in fact, tagged, and there's been a great deal of
skepticism regarding the ability to scan tags when
carried by a consumer, because of problems with UHF
tags, for instance, encountering interference from
liquids, human beings being liquids, and so on and so
forth, but we're essentially arguing about video
surveillance in the age of the daguerrotype. We don't
know exactly how this technology is going to evolve, and
there will undoubtedly be advances that will make
scanning more effective. So, let's think about the

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
implications.

We've already talked about several scenarios in which consumer privacy might be violated. This slide is an attempt to encapsulate some of the possible risks. An ordinary consumer like Mr. Jones here can be subject to scanning of a number of embarrassing items, and in some cases, of items that might actually pose a risk to his personal safety. For instance, the European Central Bank is purportedly considering plans to embed RFID tags in Euro bank notes, so you can imagine a mugger scanning for Euro bank notes and selectively mugging.

I think that the focus on databases actually over the course of the day has actually been misguided to a certain extent. The information described in this slide is actually available in the RFID tags themselves. They carry manufacturer codes and product codes in addition to unique identifiers.

The suggestion has been that people will not be able to decipher these codes because they won't be able to access the databases that contain the codes, but these codes will be standardized, and it will not take very long for somebody to figure out that 123 means Coca-Cola. It's on all of the tags, it's part of a standard, and it will be in a database that will be accessible to every single member of EPCglobal, of which
there will be hundreds.

There's also been the suggestion made that we can simply encrypt these numbers in order to protect them, but encryption is a red herring here. If you encrypt the number 1-2-3, you will get another number, perhaps it will be 8-9-7. It won't take people too long to figure out that 8-9-7 means Coca-Cola. So, encryption doesn't quite solve the problems.

There's also the suggestion that all of the data being scanned from RFID tags will be contained in databases and protected from a legal standpoint by a privacy policy, but even if the manufacturer of the replacement hip here has a very stringent privacy policy, there is still a problem if somebody else scans the replacement hip and doesn't have a privacy policy in force, and then whom is the FTC going to prosecute? Or if the gentleman is hit over the head and mugged because of the RFID tags in his Euro bank notes, who is going to be prosecuted? Those are questions that we have to contemplate.

Then, of course, there's the problem of tracking to the unique serial numbers and the possible association with consumer identities.

We've already discussed at great length over the course of the day examples of consumer backlash. I
think a particularly telling statistic, due to Ravi Pappu at Thing Magic, is that some 42 percent of the Google hits on RFID include the word "privacy."

One solution that's been proposed over the course of the day is killing of RFID tags, and this appears to make sense. If you kill the tags, of course, dead tags tell no tales, but this also I think is rather a red herring, because RFID tags are much too useful, and I'll explain why I think that is.

There's been the implication that consumer choice is going to be the most important tool to bring to bear to defend consumer privacy, but if you give consumers a choice between convenience or lack thereof -- and having RFID tags will be convenient -- of course, they'll choose the convenient option.

Moreover, suppose that consumers do choose to have live RFID tags. They shouldn't for that reason abrogate their rights to privacy.

Well, I said RFID tags are much too useful. Over the course of the day, we've seen many places in which they're employed. One we haven't seen, curiously enough, is house pets. There are some 50 million house pets in the world with RFID tags. I have a colleague, for instance, who got a cat from a shelter, and it came with an RFID tag. So, when it ran away, the cat was
scanned and successfully returned to him, and he didn't
want the cat back, but he kept getting it back.

Okay, we have had many different descriptions of
many of the wonderful applications that RFID will bring
to consumers. It's a fantastic technology with many
benefits that have to be preserved. I won't go over any
of these in depth, because we have already learned quite
a bit about them.

Okay, so, the key message here, and again, I am
going to talk about a particular technology, is that
embedding of RFID tags, if done naively, may well pose a
serious threat to consumer privacy. It's hard to
predict the exact degree and nature of that threat, but
it will undoubtedly be present, but we can mitigate this
problem with the right technology and the right
forethought. Let me give you a glimpse of how this
might work, for instance.

At RSA, in conjunction with Ron Rivest, who is
one of the inventors of the RSA CryptaSystem, for those
who are familiar with it, we have developed something we
refer to as the blocker tag. You can think of this as
itself a kind of RFID tag that creates effectively a
sphere of privacy around the consumer.

I can't give any technical detail as to how this
works due to time limitations, but the idea is that a
reader tries to scan tags it shouldn't scan, if it tries
to scan private tags, the blocker tag will effectively
spam the reader. It does this by tricking the reader
into thinking that every possible tag in the universe is
present, so the reader sees a possible collection of
items, several thousand pairs of sneakers and a bunch of
dish washers, so on and so forth, and it has to give up
scanning. That's how this works.

Of course, this would be a disaster if somebody
brought it into a supermarket and the blocker works in a
naive way, it would cause the supermarket to shut down,
but the blocker can be selective, and in particular, the
blocker can protect privacy of private items, which is
to say items that have been purchased, without
interfering with the normal scanning operation in the
supermarket.

So, this gentleman can purchase his two bottles
of merlot, the bottles can be scanned before he's
purchased them, but will no longer be subject to
scanning after he's paid for them and the bottles belong
to him, as long as the blocker is present, but the tags
will still remain alive so he can put those bottles in
his smart refrigerator and otherwise benefit from the
many wonderful features of RFID technology.

So, as I say, the blocker tag is selective, it
will work with a privacy bit embedded in RFID tags, and
to be more concrete, in a supermarket environment, all
of the tags on items on the shelf would have their
privacy bit flipped off. When a consumer purchases an
item, the bit would be flipped on, and again, the
blocker would only block those items with a privacy bit
on until the consumer decides that he or she wants to
make use of the tags.

These are essentially, these blocker tags
themselves, RFID tags. They can be very inexpensive.
They can be embedded in shopping bags, in loyalty cards,
so on and so forth. Standard integration is extremely
helpful here, and we hope that EPCglobal will support
this proposal, and in fact, there may well be a good
chance of that.

I should also say in response to critiques by
the privacy advocacy community that we've developed ways
of allowing the blocker to enable both opt-in and
opt-out approaches, so that there need not be a burden
on the consumer necessarily to carry a blocker tag if he
or she wants to achieve privacy.

We had a blocker prototype demo here today,
which I hope some of you had a chance to see, and I
should say there are many other technical approaches to
the privacy problem. There are also legislative

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
approaches, although I would agree that legislation is premature at this point.

If you want to learn more about this, here's an unofficial URL for the RSA Labs Web site. Thank you.

MS. THORLEIFSON: Thank you. Now we have some questions. First, Elliot.

MR. MAXWELL: Let me address this to Marks & Spencer, to the king of RFID. The question is -- two questions came in. Many of Marks & Spencer's policy decisions appear to be driven by UK privacy law. In the absence of similar laws in the U.S., why should Americans expect similar transparency in item-level tagging in the U.S.?

Another sort of related question was, what, if any, role did the EU privacy regulatory regime play in the arrangements that you have made with respect to RFID?

MR. STAFFORD: Okay, it's not really true to say that our policies are driven by UK privacy law, though, of course, we want to stay within the law. We would like to go a lot further than legislation in terms of what we're doing. The UK European privacy law refers to customer information. We're not about the customer. We're not actually collecting any information about the customer at all. So, we're kind of outside that part of
the law anyway.

But our policies are driven by talking to our
own staff, by talking to consumers and talking to
consumer groups, and I think that certainly within
Europe, after the issues on genetically modified foods,
after the issues on BSE, who does the consumer look to
in Europe for good advice in terms of complex
technologies? And I think that privacy groups and
consumer groups have a role to play in taking some of
these complex issues and making them simple and
highlighting what parity is required.

So, I think that what I'm saying really in
answer to the question is no, it's not just about the
law. It's going beyond the law, and legislation, of
course, is behind the real issues, I suspect.

MR. MAXWELL: Just as a follow-up question, I
assume that Marks & Spencer has a customer loyalty
program of some sort, and how do they deal with
questions of personally identifiable information in that
program?

MR. STAFFORD: We have a new -- we do have a new
customer loyalty program that's quite new. It works at
till points in our stores. I mean, we have a very, very
strict policy of never selling any data that we have on
our customers to anybody else. So, anything that M&S
happens to know about you stays within Marks & Spencer.

MR. MAXWELL: A question was raised for Paula. I trust that my retailers have little incentive to surveil me outside of the retail setting, so doesn't this alleviate the threat of RFID to privacy?

MS. BRUENING: Could you say the end of that question?

MR. MAXWELL: I trust that my retailers have little incentive to surveil me outside of the retail setting. Does this alleviate the threat of RFID to privacy?

MS. BRUENING: Outside of the -- they have little incentive outside of the -- well, I think that one of the concerns that keeps coming home to me when I hear these discussions is the way that RFID tags are potentially going to be used with loyalty cards or simply used along with credit card information to compile this kind of personally identifiable information. It's a similar kind of collection that's happening in a different way, and it's happening with a technology that I can't see, and I think that that, in itself, is a first line of concern.

I don't think it's just about what happens when you leave the store. I think it's about the practices that go on around the technology within the store. So,
I think to say that -- you know, walking out the door of
the store I don't think makes the problem run away.

MR. MAXWELL: Rob, the question says, you say
that Wal-Mart wouldn't see Mobil's data from the
SpeedPass, but won't the EPC system allow exactly that?
Aren't both firms going to be using the EPC system?

MR. ATKINSON: It's not my impression that they
would -- there may be particular codes that are in the
EPC database, but why they would have access to the
actual database from another company to look at exactly
what has been bought, where, when, who, I just don't see
that happening.

MS. BOARD: All you get from the EPC object
naming service, or ONS, it gives you direction on where
the server is that holds this information. The
information is held at the individual company. And I
want to say specifically that it's in these companies'
best interests to have incredibly secure data networks,
because they don't want their competitors to get any
information about their business. So, there is the
highest level of security for this information.

MR. MAXWELL: There's a comment that was passed
in as well from a spokesman from Procter & Gamble, and
it says, in response to Ms. Albrecht's comments, we
would like to set the record straight. Procter &
Gamble's Pantene bottle was tested in a laboratory environment only and never reached a retail environment. Procter & Gamble has always supported consumer choice to keep the tag active or to kill it.

Let me sort of follow up on a point that was raised by Ari and Rob and also from Cedric in this. The issue of choice on the part of consumers is sort of central to many of the questions about privacy. How should we think about choice if, in fact, consumers say I'm perfectly happy to have this kind of information aligned together and I trust this retailer? Does that make the privacy issues go away with respect to that consumer, or should there be rules that go beyond that if the consumer is willing to make such a choice?

Ari commented about that in terms of consumer choice, but Cedric, the rules that you propose and the like, and Rob, the comments that you made suggest that we should at least be thinking about how much do we weigh the choice that an individual consumer makes about the information that's collected or potentially collected about him or her.

MR. LAURANT: Yes, consent is very important to consumers. They must know -- for their consent to be taken as consent, they must be totally aware of what's going on with the tagging, with what kind of information
is being collected, processed later on, desimulated,
collated with other preexisting customer information.

What I can see now happening by reading the tags
that Marks & Spencer and Tesco and other companies
display to customers is that the statements are somehow
misleading. They do not explain clearly what's going
on. They do not explain clearly that the information
the customer will provide to the retailer, how that
information will be disseminated to other companies,
will be disclosed to other companies later on or might
be later on disclosed.

This is a very important part of most RFID
privacy policies that is generally not included in those
policies, is the fact that consumers should, if there is
an abuse, that their data is being disseminated contrary
to what the policy privacy establishes, they should have
access to court to have fair compensation, and that does
not exist under the current law, and I think the FTC
should very strictly sue the companies that have posted
a privacy policy if they do not comply with it.

Right now, what happens is the FTC has the
discretion to sue those companies, and the consumer does
not have access to the court if there is an abuse, a
privacy abuse.

MS. THORLEIFSON: Just one comment. The FTC
has, in fact, sued companies who have posted privacy
policies and then not followed them.

MR. LAURANT: Yes, I haven't said that, but they
have the discretion to do so, and there is no
possibility when customers' privacy is being invaded to
actually sue the company, the infringing companies,
before a court.

MR. ATKINSON: I guess my take on that, Elliot,
is that a lot of the choice discussion ends up being
framed as if choice is costless, and if you thought
about choice from the environment -- let's say
ultimately we get to the Metro smart card solution where
you can stick your card through and it automatically
gets scanned, which I'd love to have, boy, that would be
great, you could really cut the cost of products and
speed checkout.

What if somebody says I don't like that, and I
deserve choice, so I deserve to actually have my stuff
read individually by somebody who's looking at it and
looking at the price. Okay, that's going to raise the
cost of checkout a significant amount, probably add a
dollar to checkout. Is the company going to be able to
charge for that? No way. Companies simply will not
charge for that, because it's the way the market works,
and yet, who will pay for that? Pretty much everybody
else who doesn't really care.

    So, I think we've got to really be careful with choice. We have got to say, what are we actually giving people choice of? And I think the choice should be, to the extent feasible, do you remove the tag or not?

    But the sort of choice about databases I think is frankly a red herring. It's a problem in search of a solution. We don't have choice today when I go to Safeway and I use my credit card. If I don't want them to know who I am, I just pay with cash. That's the choice we make. You don't like it, pay with cash.

    MR. MAXWELL: In the post-9/11 environment, one of the observations that people have made is that information in the hands of the private sector is no longer so clearly distinguishable as information in the public sector. The use of private sector information for anti-terrorist activities and the like has tended to collapse a distinction that we used to make very clearly between information that private companies had and information that the Government had access to, and I'm wondering whether this kind of collapse of the distinction would change any of the things we do about information collection in general.

    It's not specific to RFID, but it may change how we think about the rules governing access to

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
information. I'd be interested to see whether anyone wanted to comment about that.

DR. JUELS: Well, I think that you're pointing to a larger phenomenon here, Elliot, which is the fact that the abuses of RFID may not necessarily be committed by the original owners of the RFID tag. The retailer who sells me the given item is not necessarily going to be the malefactor who abuses my privacy, and there should be concerns about abuse of RFID by local law enforcement, for instance, particularly the abuses that can take place covertly, and by retailers who may not have privacy policies in place, to reiterate an earlier point.

RFID is different than a loyalty card or a credit card in that it's not a closed system. The RFID tag can be scanned by somebody other than its original owner, and it can be scanned at times when there's no active volition on the part of the consumer.

MR. MAXWELL: But at the same time, I'm concerned that legislation, precisely because RFID, its technological facets make it such a slippery beast, that legislation may not be effective in capturing all of these nuances and really protecting consumer privacy.

Okay, I think this is going to be the last question, and I would suggest a kind of theme that's

For The Record, Inc. 
Waldorf, Maryland 
(301) 870-8025
gone throughout this, trying to figure out how RFID is
different if in any significant way from what
information consumers provide and retailers have had
access to in the past. Merchants have known the names,
addresses, items purchased, frequency of shopping,
amounts paid and lots of other stuff about their
customers since the 1800s and before. So, really, what
is new now, and what should we do differently now than
we do with respect to the information that they have had
access to and have had access to for quite some time?

            MR. ATKINSON: Nothing.

            MS. BRUENING: I'll take the other side of that.

            Well, I think it's the power of the databases and it's
            the computing power that allows the information to be
            shared and collated and mined so efficiently, and I
            think that's a lot of where -- your point about the
            porosity of a wall between public and private sector
            becomes so important, that because of that power and
            those rich dossiers that we can potentially create, our
            concerns about who has access to that become greater,
especially in the environment we're living in.

            MR. STAFFORD: I think I would just sort of like
to bring it a little bit back to in the end, the RFID
deployment by retailers and manufacturers will be driven
by very sensible and very robust business cases to make

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
the investment and to see a proper return on that investment. It's very hard to think of any scenario involving customer information that actually justifies any of this sort of investment.

There is such an enormous opportunity to use RFID to improve the efficiency and visibility of supply chains and to actually provide better customer service, but I don't think anybody really needs to go into these contentious areas, because I don't see the business case for it.

Now, of course, we should be aware about what other people could do with what we're using by accident or by design, but provided we keep thinking about the possibilities going forward and we keep trying to steer away from any negatives, then I think we've got a rosy scenario for it. But be clear, there isn't a business case about gathering customer information through RFID. The business case, the fantastic business case, is all about manufacturing efficiency and supply chain efficiency, and that's the direction the industry will take RFID in, I believe.

MR. MAXWELL: Let me then sort of make one sort of comment before we wrap up. There clearly are a couple of distinguishable issues. As people described throughout the day, there's relatively little concern in
the supply chain, per se, about the privacy issues.

There are issues in the retail store and in the retail environment which look a lot like, although not exactly like, the issues that we have with customer loyalty cards and the retention of information that's already collected.

There are a set of issues after sale which are somewhat different and for which we have less experience, and so it seems to me that one of the things that we should be talking about is how do we look carefully at the question of access to data, which goes across both the in-store sale and post-sale data, and secondly, about how we deal with the issues of access to the information potentially available via the chip post-sale, but those two places of focus are places where, again, we can think about what can be done with a technology, what can be done by industry practices, what can be done by consumer education, and potentially, what can be done by government action.

I think the FTC has been prescient in trying to get people together to talk about these issues, to begin this dialogue, which I hope will continue for quite some time as we learn from each other.

I'd like to thank the panel very much for coming, for your kind of incredible patience with the

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
amount of information you've been given, and if anyone
would like to know what my purchases are at Giant and
Safeway, they can come up and see me after.

Thanks very much.

(Appplause.)

MR. HARWOOD: I just want to mention as people
are headed out that you still have an opportunity to
comment on anything that's been said today or submit
additional comments. Comments are open until July 9th
on the FTC's Web site, which is ftc.gov/ridworkshop.
We would love to hear from you if you have more thoughts
about what we've talked about today.

I would like to thank everybody who's come today
on behalf of Director Beales of the Federal Trade
Commission, particularly thank our panelists and
particularly thank Julie Brof for putting this on.
Thank you very much.

(Appplause.)

(Whereupon, at 5:32 p.m., the workshop was
concluded.)

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025
CERTIFICATION OF REPORTER

DOCKET/FILE NUMBER: P049106
CASE TITLE: RADIO FREQUENCY IDENTIFICATION WORKSHOP
DATE: JUNE 21, 2004

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: 07/22/2004

SUSANNE BERGLING, RMR

CERTIFICATION OF PROOFREADER

I HEREBY CERTIFY that I proofread the transcript for accuracy in spelling, hyphenation, punctuation and format.

DIANE QUADE

For The Record, Inc.
Waldorf, Maryland
(301) 870-8025