

RFID TECHNOLOGY: WHAT THE FUTURE HOLDS FOR COMMERCE, SECURITY, AND THE CONSUMER

HEARING BEFORE THE SUBCOMMITTEE ON COMMERCE, TRADE, AND CONSUMER PROTECTION OF THE COMMITTEE ON ENERGY AND COMMERCE HOUSE OF REPRESENTATIVES ONE HUNDRED EIGHTH CONGRESS

SECOND SESSION

JULY 14, 2004

Serial No. 108-108

Printed for the use of the Committee on Energy and Commerce



Available via the World Wide Web: <http://www.access.gpo.gov/congress/house>

U.S. GOVERNMENT PRINTING OFFICE

95-455PDF

WASHINGTON : 2004

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512-1800; DC area (202) 512-1800
Fax: (202) 512-2250 Mail: Stop SSOP, Washington, DC 20402-0001

COMMITTEE ON ENERGY AND COMMERCE

JOE BARTON, Texas, *Chairman*

W.J. "BILLY" TAUZIN, Louisiana	JOHN D. DINGELL, Michigan
RALPH M. HALL, Texas	<i>Ranking Member</i>
MICHAEL BILIRAKIS, Florida	HENRY A. WAXMAN, California
FRED UPTON, Michigan	EDWARD J. MARKEY, Massachusetts
CLIFF STEARNS, Florida	RICK BOUCHER, Virginia
PAUL E. GILLMOR, Ohio	EDOLPHUS TOWNS, New York
JAMES C. GREENWOOD, Pennsylvania	FRANK PALLONE, Jr., New Jersey
CHRISTOPHER COX, California	SHERROD BROWN, Ohio
NATHAN DEAL, Georgia	BART GORDON, Tennessee
RICHARD BURR, North Carolina	PETER DEUTSCH, Florida
ED WHITFIELD, Kentucky	BOBBY L. RUSH, Illinois
CHARLIE NORWOOD, Georgia	ANNA G. ESHOO, California
BARBARA CUBIN, Wyoming	BART STUPAK, Michigan
JOHN SHIMKUS, Illinois	ELIOT L. ENGEL, New York
HEATHER WILSON, New Mexico	ALBERT R. WYNN, Maryland
JOHN B. SHADEGG, Arizona	GENE GREEN, Texas
CHARLES W. "CHIP" PICKERING, Mississippi, <i>Vice Chairman</i>	KAREN MCCARTHY, Missouri
VITO FOSSELLA, New York	TED STRICKLAND, Ohio
STEVE BUYER, Indiana	DIANA DEGETTE, Colorado
GEORGE RADANOVICH, California	LOIS CAPPS, California
CHARLES F. BASS, New Hampshire	MICHAEL F. DOYLE, Pennsylvania
JOSEPH R. PITTS, Pennsylvania	CHRISTOPHER JOHN, Louisiana
MARY BONO, California	TOM ALLEN, Maine
GREG WALDEN, Oregon	JIM DAVIS, Florida
LEE TERRY, Nebraska	JANICE D. SCHAKOWSKY, Illinois
MIKE FERGUSON, New Jersey	HILDA L. SOLIS, California
MIKE ROGERS, Michigan	CHARLES A. GONZALEZ, Texas
DARRELL E. ISSA, California	
C.L. "BUTCH" OTTER, Idaho	
JOHN SULLIVAN, Oklahoma	

BUD ALBRIGHT, *Staff Director*

JAMES D. BARNETTE, *General Counsel*

REID P.F. STUNTZ, *Minority Staff Director and Chief Counsel*

SUBCOMMITTEE ON COMMERCE, TRADE, AND CONSUMER PROTECTION

CLIFF STEARNS, Florida, *Chairman*

FRED UPTON, Michigan	JANICE D. SCHAKOWSKY, Illinois
ED WHITFIELD, Kentucky	<i>Ranking Member</i>
BARBARA CUBIN, Wyoming	CHARLES A. GONZALEZ, Texas
JOHN SHIMKUS, Illinois	EDOLPHUS TOWNS, New York
JOHN B. SHADEGG, Arizona	SHERROD BROWN, Ohio
<i>Vice Chairman</i>	PETER DEUTSCH, Florida
GEORGE RADANOVICH, California	BOBBY L. RUSH, Illinois
CHARLES F. BASS, New Hampshire	BART STUPAK, Michigan
JOSEPH R. PITTS, Pennsylvania	GENE GREEN, Texas
MARY BONO, California	KAREN MCCARTHY, Missouri
LEE TERRY, Nebraska	TED STRICKLAND, Ohio
MIKE FERGUSON, New Jersey	DIANA DEGETTE, Colorado
DARRELL E. ISSA, California	JIM DAVIS, Florida
C.L. "BUTCH" OTTER, Idaho	JOHN D. DINGELL, Michigan,
JOHN SULLIVAN, Oklahoma	(Ex Officio)
JOE BARTON, Texas,	
(Ex Officio)	

CONTENTS

	Page
Testimony of:	
Bruening, Paula J., Staff Counsel, Center for Democracy and Technology .	24
Dillman, Linda M., Executive Vice President and Chief Information Officer, Wal-Mart Stores, Inc	13
Galione, William, Vice President and General Manager, Marketing and Sales Americas, Philips Semiconductors	30
Hughes, Sandra R., Global Privacy Executive, Procter & Gamble Company	20
Laurant, Cédric, Policy Counsel, the Electronic Privacy Information Center	42
McLaughlin, Mark, Senior Vice President, Naming and Director Services Division, VeriSign, Inc	40
Molloy, John, Managing Director, ViaTrace, LLC	49
Sarma, Sanjay, Associate Professor, Mechanical Engineering, Massachusetts Institute of Technology	7
Steinhardt, Barry, Director of the Technology and Liberty Program, the American Civil Liberties Union	34
Additional material submitted for the record:	
Grocery Manufacturers of America, prepared statement of	66
Retail Industry Leaders Association, prepared statement of	69

RFID TECHNOLOGY: WHAT THE FUTURE HOLDS FOR COMMERCE, SECURITY, AND THE CONSUMER

WEDNESDAY, JULY 14, 2004

HOUSE OF REPRESENTATIVES,
COMMITTEE ON ENERGY AND COMMERCE,
SUBCOMMITTEE ON COMMERCE, TRADE,
AND CONSUMER PROTECTION,
Washington, DC.

The subcommittee met, pursuant to notice, at 11:36 a.m., in room 2123, Rayburn House Office Building, Hon. Cliff Stearns (chairman) presiding.

Members present: Representatives Stearns, Shadegg, Issa, Otter, Barton (ex officio), Schakowsky, McCarthy, and Strickland.

Staff present: Chris Leahy, majority counsel and policy coordinator; David Cavicke, majority senior counsel; Shannon Jacquot, majority counsel; Brian McCullough, majority professional staff member; Will Carty, majority legislative clerk; William Harvard, majority staff assistant; Jonathan Cordone, minority counsel; and Ashley Groesbeck, minority research assistant.

Mr. STEARNS. Good morning, everybody. Welcome to our subcommittee hearing entitled "Radio Frequency Identification (RFID) Technology: What the Future Holds for Commerce, Security, and the Consumer."

My colleagues, technology is only constrained by the limits of our imagination and our ingenuity. And whether it's an incremental step or the next high-tech revolution, trying to deal with the policy implications that technology brings is something that challenges us all as policymakers and legislators more frequently now than ever before. Do you have the volume up enough on this? If you can, just a little bit.

Today, I'm pleased to say that this subcommittee will attempt to get out in front and conduct the first congressional hearing on a very exciting and a complex new technology application.

As we will learn, Radio Frequency Identification, or RFID, as it is commonly known, is frankly a World War II-era technology that has begun to find new commercial and government application in just the last few years. In basic terms, the most common commercial application of RFID used radio waves to transmit data from a transmitting device called a "tag" to a scanning device called a "reader" which can be networked with a computer data base. These RFID tags can be attached to products and packaging individually.

Readers are able to activate tags via radio signals and receive tag data without “line-of-sight” scanning, which is a limitation for the common barcode. One of our expert witnesses, Dr. Sarma of the Massachusetts Institute of Technology, will provide us with a brief demonstration of RFID technology at the beginning of his testimony. It’s nice to have this room modified for this, too.

In terms of the data embedded in the tags, work is being done to develop common standards known as the Electronic Products Code or “EPC” to create unique numerical identifiers for individual items. This would allow RFID readers to receive EPC data from tags on items and products that can be matched through a data base for identification and for other purposes.

My colleagues, this is a global effort and, in theory, could lead to a seamless supply chain and logistics management in global trade. While still far off, such possibilities have led some to comment that because EPC identifies a product much like an IP address identifies a computer, RFID and EPC, in effect, are creating an internet for physical items rather than just for data. Think about that.

For manufacturing and retail applications, RFID technology is gradually being rolled out for tracking large bulk containers and pallets along the supply chain. And if technical and cost feasibility issues can be addressed, RFID readers, for example, could have the ability to read instantaneously not only pallets but also each unique individual product they contain. This could be done without having to unload any product contents, with inventory being updated in real time.

Forecasting would become obsolete, shelves would always be stocked with the most popular brands, and cost savings would be passed on to the consumer. Now this is just one possibility, future possibility. Currently, RFID technology is being used in such diverse applications as automatic traffic tolls, like the E-Z Pass system that I use when I come from my hometown to Orlando to get to the airport, and in anti-theft immobilizers on the latest automobiles.

There also are plans to use RFID technology for counterfeit drug detection as well as tracking port cargo and hazardous substances for homeland security purposes. One possible future application that seems to generate excitement for anyone who has ever stood endless in line at the grocery store, involves using readers at checkout. In this application, readers placed at checkouts would allow customers to pass straight through with their RFID tagged items loaded in their shopping carts. Customer accounts would be automatically updated leaving them free to head straight for the parking lot—without even stopping for so much as a candy bar at the checkout or buying that little magazine.

However, it is just this type of point-of-sale application that raises significant privacy issues and serious questions for average consumers and their everyday lives. To take my favorite example at the grocery store—will RFID tagged items in my cart be clearly labeled? Will I be able to disable or remove them at point of sale? What happens to the data harvested from all these purchases of myself and my family? How secure is that data, and what prevents third parties from misusing it or acquiring readers for invasive

purposes? These are all important questions and I look forward to discussing them. And it's also not just in the grocery industry. It could be in the video, Blockbusters, it could be anywhere and everywhere.

Like every new technology and application, RFID technology has the power to benefit all of us. It also presents a number of serious issues if it is misused, it could be harmful. So it is our job to cut through this hype, get the facts about RFID, learn more about its applications, and examine the public policy issues generated by its use and widespread deployment. And to help us learn more about the technology and its policy implications, we are especially pleased to have such a distinguished panel of witnesses from academia, business and consumer privacy organizations as well.

We have nine of you, I think, so we appreciate your patience here. I'd like to thank the witnesses and with that, I recognize my distinguished colleague, Ms. Schakowsky.

Ms. SCHAKOWSKY. Thank you, Chairman Stearns for holding this hearing today on Radio Frequency Identification, an old technology with new applications being discovered every day.

Once again, our subcommittee is contending with issues that arise at the intersection of technological innovation and consumer privacy. How we choose to respond to the potential uses and threats of RFID will be pivotal to consumers, civil liberties and commerce.

Although around since World War II, we are hearing about RFID, a micro chip that can transmit unique information easily, more today than ever. Most often, RFID is being touted as the technological solution to inventory and supply tracking. Using RFID tags to inventory items will allow for real time supply chain tracking and we will never have to see an out of stock sign again.

What we are also hearing about, however, are the potentially serious Orwellian possibilities of RFID technology. Because of the flexibility of RFID, suppliers and retailers are exploring the possibility of using RFID chips not only on shipping crates and pallets, but on individual items as well. It's possible to have RFID tags in everything from individual pieces of clothing as Bennetton proposed to tanks as the Defense Department is already doing.

It is also being quietly suggested as Mr. Steinhardt from the ACLU will detail in his testimony that RFID tags could be used in travel documents like passports. Soon we could have Big Brother and Big Business tuning to the same frequency for not only will they know where you are, but they'll know what you're wearing.

RFID tags can be small as a grain of sand. They can be hidden in products and documents without one's knowledge. This raises serious privacy concerns. Trials have already taken place, some without adequate consumer consent. Two companies represented here, Wal-Mart and Procter and Gamble conducted such a trial with lipstick that had RFID tags. As the Chicago Sun Times reported last year, every time a consumer would pick up a lipstick off the shelf in Broken Arrow, Oklahoma Wal-Mart, a video monitor would be triggered and images of the consumer would be sent to Procter and Gamble researchers in Cincinnati. Despite this, many attempt to downplay the threats to privacy and civil liberties. We are told that the technology to do the kind of tracking that privacy and civil lib-

erty advocates discuss does not exist. We are told that suppliers and retailers aren't interested in doing the kind of surveillance about which I am concerned, yet the example at Wal-Mart leads me to believe there may be an interest. We cannot dismiss these concerns.

As with so many of the technologies that we have discussed in our subcommittee, there are amazing positive uses for RFID. I do believe that RFID could be quite useful to follow products from manufacture to point of sale. I also believe that it could help ensure that pharmaceuticals are not counterfeit, have been handled properly en route from production to the point where they are dispensed.

I appreciate the E-Z passe and SmartCards for public transportation. As one who has been fighting waste and abuse in the Department of Defense, I am pleased to hear that DOD is using RFID to keep better track of its purchases.

However, I believe that we must not turn a blind eye to the potential for the abuse of this technology. I am not willing to sacrifice personal privacy and civil liberties. I believe that we can look into ways to regulate the use of RFID so we can help the industries that could benefit from this technology while protecting rights and liberties that are fundamental to our democracy.

Again, thank you, Chairman Stearns for convening today's hearing with witnesses covering a broad range of the different stakeholders and I look forward to hearing from all of them.

Mr. STEARNS. I thank the gentlelady and the Full Chairman, the Distinguished Chairman, Mr. Barton.

Chairman BARTON. Thank you, Mr. Chairman. Thank you for this important hearing today. I want to thank our panel. I encouraged my subcommittee chairman to have one panel or two and we have extended this one panel about as far as it can go. I don't think we could get another person at the witness table. Especially, Mr. Molloy, we appreciate your patience. You're going to get to talk in about an hour and 15 minutes, probably. We appreciate you all being here.

We know how well and how fast technology has been moving, so it's very good to have a hearing on a technology that's been around for a long time since World War II, but it's now having new ways to use it. This new old technology is RFID or Radio Frequency Identification. It works by providing a frequency-emitting tag to a product that can be detected within its range by receivers. The private sector is embracing this technology for uses in supply chain management. This may not sound exciting, but the possibilities are for countless efficiencies for the benefit of consumers, better supply management, can avoid product shortages so that our favorite items are available when we go shopping. Grocery stores will know what it's stocking and also know that they're stocking only the freshest foods that are available.

Lower costs to the manufacturer and retailer mean lower costs to the consumer. Means more competitive American products overseas. The Defense Department recognizes potential benefits. They'll be implementing the technology for its contract with its suppliers. The benefits for Homeland Security could prove to be the most important aspect of this technology to Americans, capability to track

the imports and containers will enhance our ability to monitor what's coming into our country from overseas. Similar applications related to controlled substances and hazardous materials that are shipped within our borders will provide an additional layer of security that we should all welcome.

The applications are only limited to the effectiveness of the technology and the ability to implement them in a cost-effective fashion.

However, the same benefits that improve our standard of living also trigger concerns regarding privacy. And I know that a number of witnesses today are going to testify about their privacy concerns.

Similar to the application of other technologies that have the potential to be misused, RFID technology will present policy considerations as it develops and becomes more prevailing in our lives. Before we jump to any Orwellian conclusions about the applications of this technology, this committee will continue to examine the facts and how it's going to be used and distributed. We may hold additional hearings to explore these avenues regarding the benefits and concerns in terms of privacy.

Before I yield back, Mr. Chairman, I want to say something that's not part of the written opening statement. We had a hearing yesterday in another subcommittee about security lapses at Los Alamos National Weapons Laboratory. We went through a scandal several years ago where several classified disks disappeared. There was a Select Committee established, Department of Energy and the Department of Defense agreed to change their security procedures. Everything was supposedly going to be much safer and more secure. Well last week, two more zip files just disappeared, just walked out of the building and the testimony, some of which was in closed session, we found out that the inventory practices of the Weapons Laboratory, because they have so many classified documents and equipment, is once a year. Once a year. And this material could have been missing for a year and we wouldn't have known it. They just happened to have an inventory April 28 so we know that it was in its vault on April 28.

So I'm very interested in how the technology that we're going to discuss today might be used to help us do a more current monitoring and inventory status of our classified materials because I think some of those probably need to be inventoried, if possible, on a daily basis and this technology, at least appears to hold out the promise that it might do that. So I'm very happy the Chairman is holding this hearing.

Mr. STEARNS. I thank the Chairman for the excellent example. As I pointed out earlier, there will be a demonstration by Dr. Sarma how this technology is being used.

Mr. Strickland.

Mr. STRICKLAND. No opening statement. I look forward to the testimony. Thank you.

Mr. STEARNS. Thank you. Mr. Otter.

Mr. OTTER. Thank you, Mr. Chairman. I have an opening statement which I'll submit for the record and I want to offer my apologies to the panel. I'm going to have to leave in a little bit. I hope to return later, but I will have your written testimony and I wel-

come the input that you're giving us here today. Thanks very much for being here.

[Additional statements submitted for the record follow:]

PREPARED STATEMENT OF HON. BARBARA CUBIN, A REPRESENTATIVE IN CONGRESS
FROM THE STATE OF WYOMING

Thank you, Mr. Chairman, for calling today's hearing. Today this subcommittee has the opportunity to examine an emerging consumer concern which has yet to be addressed by Congress.

I would also like to thank the many distinguished panelists who are present today. As the initial effort of Congress to address Radio Frequency Identification (RFID), I expect the testimony offered today to play a critical role in framing public sentiment regarding this important matter. I am confident the panelists who have agreed to join us today will provide a diverse scope of insight and expertise.

Although the technology associated with RFID is not a new phenomena, recent developments in the application of RFID have caught the attention of manufacturers, distributors, retailers and consumers. Wal-Mart's recently announced requirement of its top 100 vendors to attach tags to pallets is a certain harbinger that this technology may soon be a common element in the life of the average American consumer. This subcommittee has recently delved quite deeply into the matter of consumer notification of the monitoring of their internet habits, and RFID technology could eventually pose conflicts similar to those associated with Spyware. If retailers plan to develop RFID technology for use in common transactions, Congress will need to assure customers are properly notified their spending habits may be monitored. I look forward to learning today what efforts vendors and retailers are currently making to protect consumer privacy.

Of particular interest to me today is the potential use of RFID tags in food labeling. Leading homeland security experts have stated terrorist attack via our nation's food and water supplies is a feasible possibility, and RFID tags could help prevent such terrorist acts. Recent outbreaks of mad cow disease have made consumers highly cognizant of the origins of their meat supplies, and this issue has profoundly impacted many residents of the state I serve. Ranching has become a high tech industry, and I am anxious to learn today how RFID tags may be utilized in heard management. The ability to trace and monitor America's food supply will not only stabilize our nation's economy, but also bolster our homeland security.

Again, I thank the Chairman for calling today's hearing and I yield back the balance of my time.

PREPARED STATEMENT OF HON. GENE GREEN, A REPRESENTATIVE IN CONGRESS FROM
THE STATE OF TEXAS

I'd like to thank Chairman Stearns and Ranking Member Schakowsky for holding this important hearing. I know I've made this comment before in this committee, but I feel it is an important statement to keep in mind:

Technology itself is not a problem when it comes to invasions of privacy and inconveniencing consumers. My concern lies with those who may use this technology for unethical purposes.

I was a co-author of the Anti-Spam bill. I supported legislation in this committee that is designed to deter people from using spyware in ways that invade our privacy and protect consumers.

Radio Frequency Identification Technology, as many of our witnesses will attest, is a technology that has been in use since World War II. This technology has been improved over the years to a point where retailers, ports, airlines, and consumers can benefit from this technology.

I represent both Houston Intercontinental Airport and the Port of Houston. The port of Houston is the largest port in the United States by tonnage and Intercontinental Airport is the eighth busiest airport in the country. I believe RFID technology can be used to help keep our airport and port more secure, and more productive.

However, I have the same concerns with this technology as I do with SPAM and Spyware. This committee must embrace this technology for what it can do for security and commerce, yet ensure consumers are protected from those who will seek to use this technology in ways that intrude our privacy and inconvenience us.

While I commend those entities that are creating an industry standard for using this technology, I would also encourage industry to develop standards addressing the privacy issue at the onset.

This is a rare opportunity for this committee. With SPAM and with Spyware, there were already millions of Americans adversely affected by those abusing this technology. With RFID, we have an opportunity to work with those stakeholders pioneering this technology for consumer use to ensure this technology benefits consumers, improves the productivity of our ports and protects consumer privacy.

I know this is no small task. However, if we are to enhance productivity and convenience, we need to do so responsibly.

Thank you Mr. Chairman, I yield back the balance of my time.

Mr. STEARNS. With that, we'll move to our panel here and we'll go from my left to the right. Dr. Sarma, we'll let you start. The opening statements are 5 minutes. We put a clock which you should be able to see right there on the desk. It goes from green to amber to red and amber tells you you're getting near the end and red, of course, is that over time if you see that. And with so many people here and we have nine, we hope all of you will try and stay within your 5 minutes.

Dr. Sarma. And Dr. Sarma, we're not going to include your demonstration as part of your 5 minutes, so you're welcome to take a little extra time.

STATEMENTS OF SANJAY SARMA, ASSOCIATE PROFESSOR, MECHANICAL ENGINEERING, MASSACHUSETTS INSTITUTE OF TECHNOLOGY; LINDA M. DILLMAN, EXECUTIVE VICE PRESIDENT AND CHIEF INFORMATION OFFICER, WAL-MART STORES, INC.; SANDRA R. HUGHES, GLOBAL PRIVACY EXECUTIVE, PROCTER & GAMBLE COMPANY; PAULA J. BRUENING, STAFF COUNSEL, CENTER FOR DEMOCRACY AND TECHNOLOGY; WILLIAM GALIONE, VICE PRESIDENT AND GENERAL MANAGER, MARKETING AND SALES AMERICAS, PHILIPS SEMICONDUCTORS; BARRY STEINHARDT, DIRECTOR OF THE TECHNOLOGY AND LIBERTY PROGRAM, THE AMERICAN CIVIL LIBERTIES UNION; MARK McLAUGHLIN, SENIOR VICE PRESIDENT, NAMING AND DIRECTOR SERVICES DIVISION, VERISIGN, INC.; CÉDRIC LAURANT, POLICY COUNSEL, THE ELECTRONIC PRIVACY INFORMATION CENTER; AND JOHN MOLLOY, MANAGING DIRECTOR, VIATRACE, LLC

Mr. SARMA. Thank you, Mr. Chairman and thank you to the Congressmen.

Mr. STEARNS. You can just move it over. They're all portable.

Mr. SARMA. What I'd like to do is very quickly give you a description of RFID and tell you what the ECP is. Let me start by saying thank you for excellent introductions. I really wanted to show you the technology itself. Let me start by asking a very simple question which is what is RFID? And in order to explain that, I need to put up a picture. This is an RFID tag that I'm holding up. That is another type of RFID tag. An RFID tag is a chip and an antenna. It has no battery. It is simply a chip and an antenna. And the way an RFID tag works is that a reader puts out electromagnetic waves, RF waves, which then illuminate the antenna which powers the chip and the chip responds. The chip can be very small. It can be the size of a grain of sand. The tag which is both in the chip and the antenna are about the size of a credit card. So the tag is actually much larger.

In order to explain how this works, it's probably best for me to invite Mr. Tom Sharpa who is a researcher at MIT who is an expert in RFID who set up the standards in Japan to show you how a reader and a tag work together. This is an antenna attached to a reader. This is the reader. What Mr. Sharpa is holding is an RFID tag. And what I'm going to show you now on the screen is the RFID tag being read. Now the first number shows you that one tag is being read. The second number shows you how often it's being read. It's being read about 50 times. The third number which I'll describe more is something called the Electronic Product Code. It is the number in the tag. And finally, we have some technical numbers on the screen.

Now if Mr. Sharpa can walk backwards, you will see that as he walks away, the range of the tag starts hitting the limit. There's a limited range to which you can read these tags. It's about 10 feet. It varies from tag to tag. This is an evolving technology. It will get better, but it's only about 10 feet.

Now Tom, if you can come back closer. Why don't you rotate the tag, Tom? It turns out that as you rotate the tag, it becomes more challenging, depending on the style of tag. Now Tom, if you could come closer and put the tag behind your hand. It turns out that when he hides it with his hand, the range diminishes because propagation of electromagnetic waves through many materials, especially water, is somewhat limited and certainly if he put it inside his pocket or if he turned around and put it behind him, he certainly couldn't read it.

Now it doesn't mean that you can't read tags without line of sight. It is a science that is evolving. You need to tailor it and you can get it to work and you can read pallets, you can read cases, you can read cases on conveyors, but this is an evolving technology.

Thank you very much, Tom.

So with that now, let me go back to the EPC tag and this EPC term that you've heard and describe to you what it's all about. Inside the tag, inside the chip of the tag we saw a number. That is called the Electronic Product Code. And EPCglobal is an entity that is taking this number, the Electronic Product Code and taking all the standards associated with RFID tags, everything from the numbering scheme to the language the reader speaks to the tag, to the network infrastructure required to use RFID tags in the supply chain. It's taking all these elements and standardizing them so that the supply chain can be brought into the world, into the digital world, so that the supply chain which is very opaque today, can be endowed with the visibility that the internet is endowed in information.

And where is this all leading? Well, if you take the supply chain today, it's very opaque and you have problems that plague it. Like if you walk into a grocery store and Linda Dillman may be able to comment about the small—if you walk into a grocery store, 8 percent of the time for the top selling items you'll find it out of stock, 4 percent lost sales. Across the supply chain, retailers and manufacturers carry 20 weeks of inventory. Counterfeit is a \$500 billion problem today worldwide. Shrinkage theft is a \$50 billion product. And what RFID lets you do is take the supply chain and let the partners in the supply chain, the manufacturers, the shippers, the

retailers, see what's going on so they don't have to guess and second guess. Does guessing and second guessing—(a) it makes the supply chain very inefficient, and (b) it opens up loopholes for things like counterfeits and shrinkage.

And the way I think about it is just as you store money in a bank and you can go on the internet today and see how much money you have in the bank, the supply chain is actually a series of banks. A warehouse is a bank for material. And what RFID lets you do and what the internet infrastructure with RFID and EPC lets you do is log into this bank and see how much inventory you have there. What's my account balance? Do I need to transfer money from another account?

This is what RFID and EPC lets you do and by doing this, you reduce guesswork. You make the supply chain more efficient. You lubricate the supply chain and finally, you have profound impact on things like safety, health and security.

So I'll end my comments with that. Thank you very much for this opportunity to present.

And Mr. Chairman, if there are any questions, I'm happy to take them.

[The prepared statement of Sanjay Sarma follows:]

PREPARED STATEMENT OF SANJAY SARMA, ASSOCIATE PROFESSOR, MECHANICAL
ENGINEERING, MASSACHUSETTS INSTITUTE OF TECHNOLOGY

INTRODUCTION

Chairman Stearns and other members of the subcommittee, thank you for inviting me to testify today. The subject you have chosen is one of great importance to the conduct of business around the world. I am delighted to share my views.

When I say that the topic of RFID Technology—and the EPCglobal Network it makes possible—is one of great importance for business around the world, I understand the need to be as clear as possible in explaining what I mean by that. I hope that my testimony today will serve that purpose.

The new communications network—a real-time mechanism for providing visibility in the global supply chain—we are discussing will have a vast impact. It will save billions of dollars and has the potential to save many lives. It has dozens of exciting applications that are already in development—from identifying counterfeit drugs to facilitating product recalls.

What I'm talking about is a communications network that will essentially be an "Internet of products." In this network, inanimate objects—chiefly pallets or cases of manufactured goods—will have the ability to be identified wherever they are. Much as a dark room becomes luminous when lights are switched on, the historically opaque supply chains on which so much of the world's economic activity is built will become "visible." At any moment, we will be able to tell where a given shipment is, the history of its movements through the chain, the number of items in the chain, and much more.

This system represents an enormous advance over bar code technology, in part because it is not based on lasers and therefore does not require that objects be within the line of sight of the device needed to detect them. Instead, the system relies on radio waves that can be instantly interpreted by a nearby "reader" device with its own antenna. Thus, for example, a truckload of inventory delivered to a retail warehouse could be read at once instead of having to individually identify each pallet and case of product.

This system offers huge benefits to manufacturers, retailers, distributors, and—importantly—consumers. Manufacturers will be able to track high-value items, reducing shrinkage, and increasing their speed-to-market; they'll also be able to accelerate and better target their product recalls. Distributors will see their shipping and receiving processes grow in accuracy as they fall in price. Retailers will be able to monitor inventories in real time, enabling them to keep stocks fresh and cut transportation costs.

All these improvements will result in substantial benefits for the consumer. Consumers will benefit from increased product availability and faster removal of re-

called products. There's potential for increased cost savings as efficiencies gained throughout the supply chain are passed along to the consumer.

The technology also has the potential to save lives. The system can help solve the growing challenge of counterfeit drugs, for example, by offering a drug tracking and tracing capability. Improved food safety is another positive consequence, allowing manufacturers and retailers to implement product recalls swiftly and precisely, avoiding potential health consequences and improving the integrity of the world's food chain.

There will be benefits in the public sector as well, as evidenced by the key sponsorship of RFID by the Department of Defense. DOD understands the potential for more efficient purchasing and supply tracking. Other organizations are running RFID pilots in critical applications like port security.

HOW RFID AND EPC TECHNOLOGY WORK

Radio Frequency Identification (RFID) has been around since World War II, when it was used to identify friendly aircraft. Today it is used in a variety of applications from office security passes to pay-at-the-pump convenience services.

But the use of RFID on the scale now envisioned in the EPCglobal Network had to await other advances, such as the computer revolution and the Internet.

Because of these advances, it is now possible to store on a microchip a series of zeroes and ones—digital bits—that can uniquely identify trillions of different objects—the way bar codes identify many of today's products, but with potentially much more information about a particular shipment of products. This unique series of digital bits is called the Electronic Product Code, or EPC.

Attach a tiny radio antenna to this microchip and you have an EPC “tag,” a cheaper version of a toll pass which, when asked, can signal its assigned number. The tag is not transmitting information actively. Secure devices called readers that comply with global standards developed through EPCglobal send out radio frequency waves that “wake up” the tag for a short period of time, enabling it to transmit information stored on the tag—namely the Electronic Product Code. The EPC can then be matched to the specific product information contained in a corresponding database, which is accessed through a secure network: the EPCglobal Network.

With that link complete, manufacturers and their trading partners have the ability to interpret not only what the tag is directly telling them—the EPC—but all kinds of additional background information, such as when it was made and shipped, what lot it came from, and other important information related to the movement of global commerce. The inventory is completely “visible,” assuming you have permission to access the data. And, this information can be made as secure as any Internet banking application.

Security of the EPCglobal Network is of primary concern. Even in this early stage of development, significant consideration and effort has been given to developing the specifications and standards for implementing security for all aspects of the network. There are already inherent security measures built in to the network. For example, when EPC tags pass through EPC readers throughout the supply chain, the only information collected is the EPC and the time, date and location of the read. Thus, the EPC tag, in and of itself, does not communicate meaningful information. All information associated with an EPC is found in the network and is only accessible to authorized users behind firewalls, encoding and other security measures.

The process for capturing information is very similar to that used by today's bar code technology. What is different is that the technology can capture and distribute information more efficiently. For example, in a warehouse or distribution center environment, multiple tag numbers can be collected at one time through one pass and without manually locating and scanning the tag like bar codes.

The EPC tag also allows for greater depth of serialization providing the capacity to uniquely identify one product from another. And finally, the information captured can be shared in a secure manner across existing networks and information systems, enabling companies to identify where products are in the supply chain at any given point in time.

The speed at which this information can be captured, shared, and distributed has positive implications for consumers and industry alike. Consider this: the bar code, which was standardized by EAN International and the Uniform Code Council, Inc. (UCC), is scanned more than 10 billion times daily.

In the same way the bar code revolutionized the global supply chain, the EPCglobal Network promises to significantly improve the consumer shopping experience and the way organizations move goods from one place to the other. It puts

the power of RFID to work to provide better shopping experiences for consumers and to improve efficiency all across the global supply chain.

THE AUTO-ID CENTER AND EPCGLOBAL

In 1999, the Uniform Code Council, Inc. (UCC), a not-for-profit standards making body based in Lawrenceville, N.J., which had spearheaded the adoption of bar code technology, joined with Procter & Gamble and The Gillette Co. in helping establish the Auto-ID (Automatic Identification) Center at the Massachusetts Institute of Technology (MIT). Sponsorship of the center soon grew to more than 100 global companies, and research spread beyond MIT to five other great research universities around the world: at the University of Cambridge in the United Kingdom; the University of Adelaide in Australia; Keio University in Tokyo, Japan; Fudan University in Shanghai, China; and the University of St. Gallen in Switzerland. The center's mission was to develop RFID for use across the global supply chain.

The vision was simple: harness the capability of RFID to create a world in which we can effectively track products throughout the supply chain using a single, global network as products move from one company to another, one country to another. The idea behind this vision was to make it as easy for one company to read another company's "tags" as it is for IBM computers to communicate with Apple machines over the Internet.

One focus of the center's work was the development of the identification system for objects in the system—the EPC. Another was the development of the entire system in which EPC tags could be used—the EPCglobal Network.

To develop a universal, open network that can be applied across all industries and across all countries—so that individual objects could be tracked through the entire global supply chain—requires common standards and a common infrastructure, much as commonality is demanded by the Internet.

By November, 2003, enough progress had been made in these efforts to create a new organization, called EPCglobal Inc., with the mission of developing the technical standards pertaining to the EPCglobal Network and driving their adoption across industries and across the world. The Auto-ID Center at MIT evolved into the research-focused Auto-ID Lab, while EPCglobal took on what had been the center's administrative responsibilities. The formation of EPCglobal signaled the beginning of the road to the commercialization of EPC technologies.

EPCglobal is a joint venture of the UCC and EAN International, a global, Brussels-based not-for-profit organization similar in purpose to the UCC, and which played a key role in the adoption of the bar code in Europe. Such parentage provides EPCglobal with a background in user-driven standards development that is unmatched.

EPCglobal is supervised by a board of governors drawn from its parent organizations, as well as the faculty of MIT and some of its end users representing multiple industries, from healthcare to high tech to consumer packaged goods.

The organization is working collaboratively with end-users (companies implementing the technology) and solution providers (companies building the technology) to build the infrastructure for the EPCglobal Network. It is also providing comprehensive implementation support, including standards development and maintenance, education and training, and certification and compliance programs.

THE IMPORTANCE OF GLOBAL STANDARDS

The key to commercializing EPC is the development of global standards. The significance of common standards cannot be overstated. The absence of such standards today is the most prominent barrier to explosive development of the network. In the absence of common standards, organizations could incur high costs to give their products multiple-standards compatibility, leading to higher prices.

Creating an open, global network for RFID based on a set of common global technical standards means that companies investing in systems can have confidence that the EPC tags they put on their products can be read by trading partners across the country or around the world. It also means the manufacturers of EPC solutions can make equipment in vast quantities, since that equipment will work with anyone's system. These economies of scale will reduce equipment prices, giving companies an equal opportunity to reap the enormous benefits EPC can bring. All companies benefit from an open system.

A recent Capgemini report estimated that global standards can help boost productivity improvements—with 1 percent to 3 percent of supply chain costs gained. When you consider that we have a \$10 trillion supply chain, you can begin to see the magnitude of what's at stake. The improvement potential is comparable for both retailers and manufacturers, and applies to companies of all sizes.

Subscribers to the EPCglobal Network have the opportunity to participate in the development of network standards. EPCglobal, like its parent organizations, UCC and EAN International, is open and neutral, as well as highly user driven. The standards development process works through a submissions track, which is designed to ensure that business requirements are captured, and a standards track, designed to create them, test and eventually ratify them.

Much of the work is done through Working Groups and Action Groups who comprise international users from a variety of industries who are charged with defining business and technical requirements for the EPCglobal Network. Action groups, for example, help develop the foundational building blocks of the EPCglobal Network, working toward the creation of industry standards and commercial adoption.

Current action groups that have been established include:

- The Business Action Group, which is comprised of representatives from companies that currently use or plan to use EPCglobal Network technology. The group's aim is to establish business requirements and use cases across multiple industries to facilitate supply chain efficiency.
- The Hardware Action Group, which develops specifications for key hardware interface components of the EPCglobal Network, including the air, interface protocols between readers and tags.
- The Software Action Group, which creates the system software architecture and system specifications for reader management, middleware, and EPC Information Services, which connect trading partners for secure data queries.

This thorough and collaborative standards development process is open and inclusive. The organization leads a neutral, consensus-based process where every company has the opportunity to contribute.

PUBLIC POLICY CONSIDERATIONS

For the EPCglobal Network to reach its full potential, certain protections must be built into the system. It is EPCglobal's position that addressing concerns, such as consumer privacy, is as important as anything the organization is doing. Reflecting that understanding, the sponsors of the network adopted guidelines for use by all companies engaged in the large-scale deployment of EPC. These guidelines are intended to complement the national international laws and regulations dealing with consumer protection, consumer privacy, and related issues. The guidelines state:

- Consumers will be given **clear notice** of the presence of EPC on products on their packaging.
- Consumers will be **informed of the choices** they have to discard, disable, or remove EPC tags from the products they acquire. (It is anticipated that for most products, the EPC tags would be part of disposable packaging or would be otherwise easy to discard.)
- Consumers will have the opportunity to **easily obtain information** about EPC and its applications, as well as information about advances in the technology. Companies using EPC tags at the consumer level will cooperate in appropriate ways to familiarize consumers with the EPC logo and to help consumers understand the technology and its benefits.
- Companies will **use, maintain, and protect records** generated through EPC in compliance with all applicable laws.

These guidelines demonstrate that EPC participants are committed to addressing the issue of consumer privacy and engaging in a constructive and on-going dialogue with interested parties. The overriding goal of the guidelines is to provide a responsible basis for the use of EPC tags on consumer items. Under the auspices of EPCglobal, these guidelines will continue to evolve as advances in EPC and its applications are made and consumer research is conducted.

To foster continued dialogue with key audiences about public policy and other important areas, EPCglobal and some of the industry sectors with which it's working have also formed the EPC Public Policy Steering Committee (PPSC). The committee and its working groups will include representatives of industries and trade associations worldwide, from healthcare, technology, food, consumer products, retail and others. The PPSC owns responsibility for the Consumer Policy Guidelines and will be working closely with industry, consumers, and government leaders to communicate the benefits of the technology, as well as understanding the complex issues surrounding consumer privacy.

CONCLUSION

The EPCglobal Network will be focused on the supply chain—and, in the first few years, almost entirely at the case and pallet level, in factories, back-rooms, distribu-

tion centers, and warehouses. As the price of implementation falls, EPC applications will spread to the consumer unit level, where it can be used to manage shelf inventory and identify counterfeit products.

The savings to the economy will be significant. Accenture, a consulting firm, estimated that RFID could eliminate 15 to 30 percent of missing inventory. Estimates are that the retail industry alone loses more than \$50 billion a year to theft, paperwork errors, and vendor fraud. Product counterfeiting costs another \$500 billion a year worldwide. At the same time, it's estimated the technology can increase revenues by 1 to 2 percent, by reducing out-of-stock items.

Consumers should benefit from these reduced costs. And, in the case of product recalls, the merchandise can be tracked quickly. Their medicines will more likely be genuine; today, according to the World Health Organization, 7 percent of global pharmaceuticals are counterfeit.

As with any technology, however, it is impossible to anticipate the full spectrum of uses to which RFID Technology and the EPCglobal Network will be placed. This testimony has been focused entirely on the supply chain, because that is where the interest primarily now lies and what the current technology is capable of providing.

Thank you for the opportunity to present EPCglobal's position on the many benefits associated with this exciting technology and the organization's commitment to protecting consumer privacy.

Mr. STEARNS. And I thank you.
Ms. Dillman.

STATEMENT OF LINDA M. DILLMAN

Ms. DILLMAN. Good morning, Mr. Chairman, members of the committee. I have submitted written testimony to go in the record. If I may, I'd like to read a summary of that testimony.

Mr. STEARNS. Sure, sure. All of your statements are part of the record by unanimous consent and they're all in there and if you want to read them, you can, or you don't have to.

Ms. DILLMAN. I'm the Executive Vice President and Chief Information Officer for Wal-Mart. Wal-Mart is the Nation and world's largest retailer, with facilities in all 50 states and 10 countries. Wal-Mart was the first retailer to join MIT's AUTO-ID lab in 1999 because we recognized that RFID had the potential to reduce out of stock conditions through the introduction of what has now become known as an Electronic Product Code or EPC.

In July 2003, we asked our top 100 suppliers to begin using RFID tags on cases and pallets of products destined for our North Texas Distribution Centers by January 2005. It's important to note that we chose to focus on case and pallet level tagging. We did not and are not requesting item level tagging.

On April 30, 2004, Wal-Mart moved EPCs from our laboratory environment to an actual field pilot program. Currently, we have cases and pallets of 21 products from 8 suppliers destined for 1 distribution center and 7 super centers in North Texas being tagged.

While the pilot is less than 2 months old, we have found that EPCs help us gain visibility into the supply chain process and improve our merchandise availability. We are so confident in the application of this technology that we have asked our next top 200 suppliers to begin tagging cases and pallets of product by January 2006.

We further expect to have all of our more than 20,000 domestic suppliers participating in the program within the next 30 months.

Retailers such as Wal-Mart focus significant effort on ensuring items are in stock and ready for sale. During peak shopping times, such as a Saturday afternoon, it is a challenge to keep items that sell quickly like health and beauty aids in stock and actually on

the shelf. With RFID tags attached to the cases and readers placed strategically throughout the stores back room, we can tell the last reader that a case went by and to help us determine whether the case went out to the floor to be stocked or it's still in the back room.

Concerns have been raised about potential privacy abuses with RFID technology. Wal-Mart is committed to protecting the privacy of our customers. There is no additional information about individuals, available or collected, via RFID because Electronic Product Codes identify products and not people.

During 2004 to 2006, Wal-Mart will continue to focus on case and pallet level tagging. However, because some cases also serve as consumer packaging, there will be instances where a consumer could purchase a product which bears an RFID tag. We have currently three products in our pilot program that are exactly that, two HP printers and one HP scanner. Because of that, we have ensured that the tags are on the outermost packaging, so not on the product itself and adhering to the EPC global privacy guidelines are marked with an EPC global symbol.

Additionally, we place signage near the front doors of our stores participating in the pilot, more signage on the shelves where the products are sold, and we placed tearaway leaflets that provide additional consumer education on EPCs on the same shelf. The leaflets explain the project and inform consumers that they have the option to keep the tag or discard it at any point post-purchase.

Currently, EPCs will help us address the merchandise availability issue. In the future, EPCs have the potential to help us minimize wait time at checkouts, expedite returns and warranty processing and more effectively handle recalls. They also have the very real potential to make substantial progress in the fight against counterfeit pharmaceuticals. To realize all of these benefits to the fullest extent possible, however, EPCs will ultimately need to move to the individual item level. We believe that's at least 10 years away.

As the Chief Information Officer for Wal-Mart, I spend a great deal of time working to ensure the privacy of our customers. There is definitely an inherent responsibility for companies using RFID to address privacy issues. We believe that's best done through adherence to the EPC global guidelines which champion consumer notice and consumer choice.

As you review the potential of RFID technology, the most effective action that Congress could take is to underscore to any organization employing the technology that the substantial privacy protections already in place are not to be ignored in written or as in spirit. It's also important for Congress to support EPC global efforts to ensure a single global standard for RFID technology so that American companies can effectively compete around the world and American consumers can receive all the potential benefits.

Thank you.

[The prepared statement of Linda Dillman follows:]

PREPARED STATEMENT OF LINDA DILLMAN, EXECUTIVE VICE PRESIDENT AND CHIEF INFORMATION OFFICER, WAL-MART STORES, INC.

On behalf of Wal-Mart Stores, Inc., I appreciate the opportunity to provide written comments to the House Committee on Energy and Commerce Subcommittee on

Commerce, Trade and Consumer Protection concerning the expansion of radio frequency identification (RFID) technology into new industries and the potential impact on consumers.

Based in Bentonville, Arkansas, Wal-Mart is the nation and world's largest retailer, with facilities in all 50 States and 10 countries. The Company operates more than 3,030 discount stores, Supercenters, Neighborhood Markets and more than 530 SAM'S CLUBS in the United States. Internationally, the Company operates in Argentina, Brazil, Canada, China, Germany, Mexico, Puerto Rico, South Korea, and the United Kingdom. Wal-Mart also owns a 37.8 percent interest in Seiyu, Ltd, a leading retailer in Japan with options to purchase up to 66.7 percent of that company. Wal-Mart employs more than 1.2 million associates in the United States and more than 300,000 internationally.

INTRODUCTION AND OVERVIEW

As a leader in the use of technology to enhance the consumer experience, Wal-Mart was the first retailer to become involved with RFID technology. Our interest is focused around developing a method by which to improve the efficiency of our supply chain.

It should be noted that RFID technology is not new. In fact, it was first employed during World War II when it was used to help identify allied planes from opposition aircraft. Over the past half century, many consumers have come to use RFID technology—most recently in cashless toll booths and keys that significantly reduce automobile theft.

Many industries, including retail, have been keeping abreast of these developments to learn if RFID technology can help solve existing challenges that continuously frustrate customers, including lost baggage during air travel and out-of-stocks when shopping at a retail outlet. Today, through the hard work of the Massachusetts Institute of Technology's (MIT) AUTO-ID Center and its successor, EPCglobal, along with the support of companies like Wal-Mart that have encouraged their research, it is clear that RFID technology can help companies solve these problems.

Wal-Mart's efforts are focused on trying to enhance the customer experience inside the store. It is important to understand that Wal-Mart does not adopt a technology and then create uses for it. Instead, we seek technology to help us tackle existing and potential challenges that prevent us from delivering complete customer satisfaction.

HOW WAL-MART BECAME INVOLVED

Wal-Mart was the first retailer to join MIT's AUTO-ID Center in 1999. We, along with others, funded research on the potential of using RFID in the retail and consumer packaged goods sector. We began testing in 2000 and after reviewing the state of this technology in 2001, we created our own RFID lab in Rogers, Arkansas. We did our own research in addition to supporting the AUTO-ID Center. We consulted with experts. We reviewed RFID uses already in place. We did all of this to determine whether this technology could help us solve the merchandise availability issue. We recognized after reviewing RFID that it had the potential to significantly help reduce out-of-stock conditions through the introduction of what has now become known as an Electronic Product Code or EPC. In June 2003, convinced that it could, we challenged our top 100 suppliers—representing some of the most innovative companies in America—to begin using RFID tags on cases and pallets of products destined for our three North Texas distribution centers by January 2005. These distribution centers ship products to 150 of approximately 3500 Wal-Mart stores. It is important to note that we chose to focus on case- and pallet-level tagging. We did not, and are not, requesting item-level tagging.

We believe this challenge not only set direction for a new era in merchandise availability but also spawned a new market for technology companies, both those long established and others in their infancy, to be at the forefront of this revolutionary effort. Since Wal-Mart announced its EPC goals, other retailers, such as Albertsons and Target, have announced similar projects as well. The U. S. Department of Defense has also announced a similar RFID initiative.

On April 30, 2004, Wal-Mart moved EPCs from the laboratory environment to an actual field pilot program. Currently, cases and pallets of 21 products¹ from eight

¹The products include various brands of computer printers, scanners, paper towels, lotion, cat food, shampoo, feminine hygiene products, laundry detergent, deodorant, shaving cream, soap, toothpaste, and peanuts.

suppliers² destined for one distribution center and seven Supercenters³ in North Texas are being tagged. At our Sanger, Texas, distribution center, we have placed readers at our receiving doors, above our conveyor belt systems, and at our shipping doors. At the seven Supercenters, we have placed readers at the receiving doors, at strategic points throughout the stores' backrooms, at the door to the sales floor, and at the trash compactor. There are no readers on the sales floor, at the check stands, or at customer entryways or exits. The readers assist Wal-Mart in knowing when a product is received, where it is stored, when it goes out to the sales floor, if it returns for any reason, and when the case is submitted for recycling. This information is shared with our suppliers to assist them with their inventory planning.

While the pilot is less than two months old, it has demonstrated that EPCs can help us gain additional visibility into the supply chain process and improve merchandise availability. We are so confident in the application of this technology, that we have challenged our next top 200 suppliers to begin tagging cases and pallets of products by January 2006. We further expect to have all of our more than 20,000 domestic suppliers participating in the program within the next 30 months.

THE NEED FOR MULTI-INDUSTRY STANDARDS

With the introduction of any new technology there are factors that can accelerate its adoption rate. At the heart of this is the need for multi-industry standards. While you will hear more about the technology itself from others here today, let me share that, in the simplest terms, an EPC can be thought of as a better barcode, a staple of retail that just celebrated its 30th anniversary last month. An EPC contains the same Universal Product Code (UPC) number as a barcode plus a specific identifier—a license plate, if you will—that allows us to tell one box of product from another, something that could prove especially useful during product recalls. Another potential future use of this tag will be in tracking food safety and ensuring that fresh and frozen items have been maintained at safe temperatures from the time the package is prepared, through the distribution process, to the time that is sold to the consumer.

Electronic product code information is stored on a microchip that is then attached to a tag that also includes antennae. The RFID tags carrying the EPC at Wal-Mart are passive tags, meaning they contain no internal power source. A "reader" sends radio waves to the tag, activates the chip, and allows it to then transmit its data back to the reader and onto the appropriate internal computer system. The reader is an FCC Part 15 compliant device that transmits with only 1 watt per channel. Wal-Mart is using the 900 MHz radio frequency range for our case and pallet deployment. This radio frequency is similar to those used by some cordless telephones. The Federal Communications Commission regulates both the wattage and the frequency spectrum assigned to the readers and tags.

We can look to the implementation of the bar code in the retail and consumer package goods sectors and learn an important lesson. The creation of an international body to develop multi-industry standards is critical for the adoption rate. You will hear more today about EPCglobal, the organization that was formed in 2003 for these purposes. It is a not-for-profit organization entrusted by industry to establish and support the Electronic Product Code (EPC) Network as the global standard for immediate, automatic, and accurate identification of any item in the supply chain of any company, in any industry, anywhere in the world. The retail industry needs low-cost tags for the limited amount of data that is recorded and transmitted during the supply chain process. The creation of an international standards body is the foundation.

MERCHANDISE AVAILABILITY

Retailers must insure that any item is in-stock and on the shelf when the consumer is ready to purchase it. Today, we know how many items are in the store, but we do not know where they are located. Fully one-third of our inventory in a store is not on the shelf. It may be at the receiving dock and in the process of being unloaded. Thousands of items may be stored in the mini-warehouse in the back of the store. Some of them may have been temporarily relocated to another area for space reasons. Today we do not have an adequate ability to know whether those cases were taken out to the sales floor or placed on a storage shelf.

²The eight suppliers are The Gillette Company, HP, Johnson & Johnson, Kimberly-Clark, Kraft Foods, Nestlé Purina PetCare Company, The Procter & Gamble Company, and Unilever.

³Specifically in the communities of The Colony, Decatur, Denton, Hickory Creek, Lewisville, and Plano.

During peak shopping times, such as Saturday afternoon, it is a challenge to keep items that sell very quickly, such as health and beauty aids, in stock and on the shelf. Wouldn't the consumer have a better shopping experience if the stock clerk was notified in time to avoid an out-of-stock condition and where to find the replacement merchandise? With RFID tags attached to the cases and readers placed strategically throughout the store's backroom, we can tell the last reader those cases passed by, helping us determine whether the cases went out to be stocked or are just 15 feet away from the dock door through which they arrived.

The lack of merchandise availability at the point of sale, referred to as "out-of-stock" in the retail industry, is a tremendous opportunity. According to a study of this issue done by Emory University in 2002, the average retailer loses 4 percent of its sales due to out-of-stock conditions. An empty shelf represents disappointment and frustration to the consumer, a lack of a sale for both retailer and the supplier, and the potential loss of future business for that particular store and product brand. Retailers, such as Wal-Mart, focus significant effort on ensuring items are in-stock and ready for sale. We recognize that the entire supply chain process needs to be optimized. There is room for improved efficiencies in distribution centers as well as in the store's receiving process. The ability to track items through-out the supply chain will provide benefits to the suppliers and their upstream manufacturers. The fact that the issue remains a challenge for the industry demonstrates that more needs to be done and that it must be a collaborative effort involving retailers, suppliers, and technology providers.

CONSUMER PROTECTION AND PRIVACY

Concerns have been raised about potential privacy abuses with RFID technology. It has been said that retailers, for example, will be able to track customers and know when they open a can of soda inside their homes. Opponents of this technology are wrong for two reasons. First, the technology does not exist for a retailer to drive through a neighborhood, 40 feet from a home, and read passive RFID tags—the kind being used by the retail industry—through walls. The power required to generate such a read could end up destroying the tag if it were even able to reach it. Second, and more importantly, there is no desire on the part of retailers to be able to do that. Our efforts are focused on trying to enhance the customer experience inside the store. Wal-Mart is committed to protecting the privacy of our customers. There is no additional information about individuals available or collected via RFID because electronic product codes identify products, not people.

During 2004 to 2006, Wal-Mart will continue to focus on case-and pallet-level tagging. However, because some cases also serve as consumer packaging⁴, there will be instances where a consumer could purchase a product which bears an RFID tag. We currently have three products in our pilot program—two HP printers and one HP scanner—where this is the case. These tags are on the outermost packaging of the product and, adhering to EPCglobal privacy guidelines, are marked with an EPCglobal symbol. Additionally, we have placed signage at the front doors of our stores participating in the pilot, more signage on the shelves where these products are sold, and we have placed tear-away leaflets that provide additional consumer education on EPCs on those same shelves. The leaflets explain the project and inform consumers that they have the option to keep the tag or discard it at any point post-purchase.

The local Dallas/Fort Worth news media has spoken independently with customers visiting these stores about Wal-Mart's EPC effort. Those interviews⁵, which can be culled from the papers and TV broadcasts, reveal that consumers are open to the new technology and the benefits it can bring them.

Currently, EPCs will help us address the merchandise availability issue. In the future, EPCs have the potential to help us minimize wait times in checkout lines, expedite returns and warranty processing, and more effectively handle recalls. They also have the very real potential to make substantial progress in the fight against counterfeit pharmaceuticals. In fact, Wal-Mart is currently working on a small trial to track Class II pharmaceuticals with several prominent pharmaceutical suppliers and in cooperation with the Federal Drug Administration.

To realize all of these benefits to the fullest extent possible, EPCs will ultimately need to move to the individual item level. However, that is at least 10 years away. First, technology prices must come down such that it is economically feasible to place a tag on a 20-cent package of chewing gum. Second, mass adoption of the tech-

⁴This is especially true for electronic items such as televisions and computer equipment. It also is true for large products such as lawnmowers and bicycles.

⁵Specifically the May 6th KXAS-TV NBC Channel 5 broadcast.

nology will be required to achieve a benefit at the check stand. And third, consumers will have to embrace the technology.

The concerns mounted to RFID by privacy groups are reminiscent those associated with the birth of the barcode 30 years ago. If you remember back then, there were concerns about the barcode being able to track data and how prices would no longer be marked on shelves but rather made available to consumers only upon checkout. Those fears proved unfounded.

As Chief Information Officer for Wal-Mart, I spend a lot of time working to ensure the privacy of our customers⁶ (see attached). We do not seek to gather huge amounts of personal data about our customers. Instead, our focus is on trying to do correctly the most basic of things: Have the right merchandise on the shelves when customers want to buy it at a price they can afford in places convenient for them to shop. EPCs and RFID will help us do that.

There is definitely an inherent responsibility for companies using RFID to address privacy issues. We believe that is best done through adherence to existing EPCglobal guidelines, which champion consumer notice and consumer choice. EPCglobal has established a Public Policy Advisory Committee. This committee maintains, reviews and updates EPC Guidelines, develops an effective oversight role in conjunction with the proper use of EPC Guidelines and dialog with consumer advocacy groups. Committee membership is made up of senior level executives from companies deploying EPC and an independent privacy expert. The committee reports directly to the CEO of EPCglobal who is invited to all meetings. The committee involves both retailers and manufacturers and is geographically dispersed.

CONCLUSION

As you review the potential of RFID technology, the most effective action that Congress could take is to underscore to any organization employing RFID technology that the substantial privacy protections already in place are not to be ignored as written or in spirit. It is also important for Congress to support EPCglobal efforts to ensure a single global standard for RFID technology so that American companies can effectively compete around the world and so that American consumers can receive all of the potential benefits this technology has to offer.

Wal-Mart appreciates the opportunity to present our views. We are prepared to assist members of the Subcommittee in any manner as it continues to consider the important impact RFID technology will have on American consumers.

WAL-MART STORES, INC. PRIVACY POLICY FOR CUSTOMERS AND MEMBERS

One of Wal-Mart's Three Core Basic Beliefs is "Respect for the Individual." Accordingly, we (Wal-Mart Stores, Inc. and our Affiliates—SAM's Club, Walmart.com, Samsclub.com, and any other companies in which we have a majority ownership interest) will collect and use personal information of customers and members only as follows:

Our purpose in collecting personal information.

Personal information means information about you which is, or can be, tied to you as an individual.

We collect personal information to:

- deliver the products and services you want;
- administer our businesses;
- develop and communicate special offers;
- provide customer service; and
- respond to legal process (such as subpoenas and warrants).

What information we collect and how we collect it.

The information we collect may include:

- contact information, identification numbers, account numbers, product preferences, and other information you provide when you do business with us, either online, in our stores, or at our membership warehouse clubs, or sign up for certain services, such as a gift registry or personalized website account;
- technical information (such as your Internet Protocol address, your computer's operating system and browser type, and the address of a referring website, if any, and the path you take through our web pages) when you visit our websites; and

⁶Wal-Mart's complete Privacy Policy can be found at www.walmartstores.com under the link Privacy and Security.

- financial and health care information provided by you and third parties (such as credit bureaus, health care providers, insurers, etc.) in connection with your transactions.

When you visit our websites, we may place a “cookie,” a small computer file, on your computer to help us recognize and serve you better when you return. You may delete this cookie from your computer. You may also set your Internet browser to reject cookies, however, doing so may limit the functionality of our websites.

At some stores and clubs we may record your presence on security monitors for safety and security purposes.

How we use personal information.

We do not sell or rent personal information to others.

We do not use cookies to track movements on websites other than our own.

We do not disclose personal information to non-Affiliates except in the following situations:

- when you request or give us permission to do so;
- when we use service providers and contractors (such as credit card issuers, check cashing bureaus, or data processors, mailing and fulfillment houses, customer service or research companies, etc.) for limited purposes to assist us in completing our transactions with you, maintaining or conducting our business, or doing customer research;
- when appropriate to prevent harm or injury (such as for product recalls, preventing fraud, or handling claims or other liabilities), or to comply with valid legal process and applicable laws.

We may share information with Affiliates for these same reasons and also to let you know about special offers, new products and services, Rollbacks, and other great values, unless such sharing is prohibited by law. We may share with Affiliates and non-Affiliates statistical information that does not identify you individually.

We take reasonable steps to protect your personal information.

We maintain reasonable physical, technical, and procedural measures to limit access to personal information to authorized individuals with appropriate purposes.

Financial, health care, and international data.

- Financial Information: If you are a check cashing customer, you will receive a separate policy concerning personal information we receive in that relationship.
- Health care information: In addition to the policies discussed above, we have more detailed information about how we handle your health care information in our Notices of Health Care Information Privacy Practices. Wal-Mart has a separate Health Insurance Portability and Accountability Act (HIPAA) Privacy Policy that is available by contacting the addresses listed below.
- International customers and members: If you provided information to us from a country other than the United States, your information may be transmitted to, and processed by us or our service providers in the United States or other countries other than your own. If you provided information from a country that grants specific additional privacy rights, contact us at the addresses listed below to exercise your rights.

Modifications to our privacy policies.

We reserve the right to change our privacy policies at any time, except as may be prohibited by law. We will post revisions online and in locations in our stores and clubs that we consider appropriate. Use of our websites or services or the purchase of products after posted changes means that you consent to the privacy policies as changed.

Contact us for more information about our privacy policies.

If you have questions about our privacy policies, contact us at privacy@wal-mart.com or Wal-Mart Stores, Inc., Attention: Privacy Office, 702 S.W. 8th Street, Bentonville, AR 72716-0860.

Mr. STEARNS. Thank you.

Ms. Hughes, welcome.

STATEMENT OF SANDRA R. HUGHES

Ms. HUGHES. Thank you, Chairman Stearns and members of the subcommittee for the opportunity to testimony today on this important issue. My name is Sandy Hughes and I am the Global Privacy

Executive for the Procter & Gamble Company. I oversee P&G's global privacy program and am a member of P&G's Electronic Product Code team or EPC team.

As background, Procter & Gamble manufacturers and markets over 300 consumer product brands to people in 140 countries. These brands include Tide, Crest, Pantene, Pampers, Vicks, Olay and Prilosec. Hopefully, you recognize a couple of those. We have over 90,000 employees worldwide and are headquartered in Cincinnati, Ohio.

Procter & Gamble is pursuing the use of Electronic Product Code or EPC to create efficiencies in the supply chain.

Today's supply chain systems are outdated and not meeting the needs of our consumers. It is frustrating when you go to your local supermarket to buy your favorite flavor of Pringles and the shelf is bare. It can result in a lost sale for P&G and for the retailer. Theft and counterfeiting are growing problems as well. Worldwide theft costs retailers \$50 billion a year and counterfeiting is a \$500 billion problem.

Since the inception of EPC in 1999, we have moved from the laboratory to testing the technology in real world supply chain situations. We are conducting pilot tests with pallets and cases with partners Wal-Mart and Target in the U.S. and Metro in Europe. In this test phase, we are still working to resolve technical issues with EPC. For example, the speed at which tagged cases and pallets pass by readers as well as the type of products, such as liquids and metallic packaging, affect the readability and reliability of the technology to read information about the product.

P&G is also a member of a pharmaceutical industry group supported by the FDA, to test how EPC can help prevent drug shortages and counterfeiting and make product recalls easier and more efficient. EPC is a powerful tool to deal with expiration date management, diversion, reduction in medication errors, product security and consumer safety, all important issues for the pharmaceutical industry.

Down the road as P&G learns more about the technology, there may be opportunities to eliminate costs and generate additional benefits for the supply chain and consumers through item level tagging. We believe it will be several years before the technology is affordable enough and the benefits great enough to be used on individual consumer product items. Like any new technology, as has been the case with the internet, responsible use requires considerable forethought by those developing and using the technology. That is why we have worked at these early stages to address privacy concerns associated with item level tags.

P&G recognizes that in order for consumers to accept EPC, they must understand the benefits for them and be confident that their privacy will be protected. P&G has a long history of responsible treatment of personal information and commitment to good privacy practices. As a consumer products manufacturer, we rely on information about our consumers to better understand their needs in order to produce superior products, information and services to meet them. P&G has an enormous stake in fostering an environment of trust in which consumers confidently share their information with us. Creating this climate of trust includes making sure

that our practices meet or exceed consumer expectations and contributing to industry and policy initiatives that enable other companies to do the same.

I must emphasize that EPC tags do not contain or collect personal information, nor are they intended to. But there is a perception that the technology could be used in this way. That is why we are working so hard to educate consumers about the facts versus the myths surrounding EPC.

We worked with our EPC global partners to craft usage guidelines for item level EPC in the fall of 2003. To complement these guidelines, P&G's internal position based on the pillars of fair information practices are as follows: Clear and accurate notice should be provided where EPC is being used and consumers should be informed as to whether products they are buying contain EPC tags. Consumers should have a choice to permanently disable or discard the EPC tag on products that they buy and this should be done without incurring cost or penalty. They should also have a choice as to whether personally identifiable information about themselves is electronically linked to the EPC number on products they buy beyond what is done with barcodes today.

We will not pursue item level tagging with partners who are not able to ensure privacy protection for consumers. We serve consumers. To do otherwise would not meet our core mission or business objectives.

P&G is informing our consumers about the pilot tests we are conducting. Up-to-date information about current tests, locations, brands and type of test, whether it's a pallet/case or case/item, can be found on our company website at www.pg.com. And I would be happy to address the Congresswoman's issues about the lipstick test during Q and A.

In any pilot where a consumer could come in contact with an EPC tag, P&G affixes a label to the case that notifies the consumer of the presence of the tag. P&G, along with other end users and EPCglobal have participated in a Federal Trade Commission workshop on RFID. The FTC has played an important role in educating consumers on issues such as safe internet surfing, on-line shopping tips and protecting consumers against ID theft. We are enthusiastic about the potential for FTC to contribute to consumer education and outreach on RFID as well.

In summary, I want to emphasize that EPC is in the early stages of development. The success of EPC depends on collaboration, global standards and affordable technology. We need the on-going support and involvement of retailers, manufacturers and other industry bodies to adopt the EPC system. EPC must become the single global standard in order for the full efficiencies of the technology to be realized and we believe the U.S. Government can help with this.

Procter & Gamble is working hard to ensure that EPC will be a win-win for all.

Thank you.

[The prepared statement of Sandra R. Hughes follows:]

PREPARED STATEMENT OF SANDY HUGHES, GLOBAL PRIVACY EXECUTIVE, THE
PROCTER & GAMBLE COMPANY

Thank you, Chairman Stearns and members of the Subcommittee, for the opportunity to testify today on this important issue. My name is Sandy Hughes and I am Global Privacy Executive for The Procter & Gamble Company. I oversee P&G's global privacy program and am a member of P&G's Electronic Product Code (EPC) team.

As background, Procter & Gamble manufactures and markets over 300 consumer product brands to people in 140 countries. Two billion times a day, P&G brands touch the lives of people around the world. These brands include Tide, Crest, Pantene, Pampers, Vicks, Olay and Prilosec. We have over 90,000 employees worldwide and are headquartered in Cincinnati, Ohio.

I will briefly explain why P&G is investing in Electronic Product Code technology and how we are using EPC. We are currently in the early phases of testing and learning about the costs and benefits of the technology and we are working to gain consumers' confidence and trust in EPC and ensure that their privacy is protected.

WHY P&G IS INVESTING IN EPC

Procter & Gamble is pursuing the use of Electronic Product Code (EPC) to create efficiencies in the supply chain. As you have heard from Dr. Sarma, EPC is a way to uniquely identify a pallet, case or individual product using radio frequency identification (RFID) technology. It's similar to today's bar code, but with many more potential uses and benefits. P&G is a founding sponsor of MIT's Auto-ID Center because we realized the enormous potential to improve processes in the entire supply chain—from our plants to retail distribution centers to store shelves. The real time, automated, accurate information that EPC generates will benefit manufacturers, retailers, suppliers and most importantly, consumers.

Today's supply chain systems are outdated and not meeting the needs of our consumers. EPC offers potential solutions for problems like out-of-stocks, theft and counterfeiting, as well as reducing inventory levels. We know that out of stock levels are higher than we, our retail partners and our consumers want. It is frustrating when you go to your local supermarket to buy your favorite flavor of Pringles and the shelf is bare. It can result in a lost sale for P&G and for the retailer. To guard against out of stocks, we keep an average of 65 days worth of product inventory, which costs us \$3 billion a year. Theft and counterfeiting are growing problems as well. Worldwide theft costs retailers \$50 billion a year and counterfeiting is a \$500 billion problem.

TESTING AND LEARNING ABOUT EPC

Since the inception of EPC in 1999, we have moved from the laboratory to testing the technology in real world supply chain situations where we are conducting pilot tests with pallets and cases with partners Wal-Mart and Target in the US and Metro in Europe. The technology is still evolving and we are continuing to learn about EPC. In this test phase, we are still working to resolve technical issues with EPC. For example, the speed at which tagged cases and pallets pass by the readers as well as the type of products, such as liquids and metallic packaging, affect the reliability of the technology to read information about the product.

P&G is also a member of a pharmaceutical industry group, supported by the FDA, to test how EPC can help prevent drug shortages and counterfeiting and make product recalls easier and more efficient. EPC is a powerful tool to deal with expiration date management, diversion, reduction in medication errors, product security and consumer safety, all important issues for the pharmaceutical industry.

Down the road as P&G learns more about the technology, there may be opportunities to eliminate costs and generate additional benefits for the supply chain and consumers through item level tagging. We believe it will be several years before the technology is affordable enough and the benefits great enough to be used on individual consumer product items. *Like any new technology, as has been the case with the Internet, responsible use requires considerable forethought by those developing and using the technology.* That is why we have worked at these early stages to address privacy concerns associated with item level tags.

PRIVACY ISSUES

P&G recognizes that in order for consumers to accept EPC, they must understand the benefits for them and be confident that their privacy will be protected. P&G has a long history of responsible treatment of personal information and commitment to good privacy practices. Why? As a consumer products manufacturer, we rely on in-

formation about our consumers to better understand their needs in order to produce superior products, information and services to meet them. As a result, P&G has an enormous stake in fostering an environment of trust in which consumers confidently share their information with us. Creating this climate includes making sure that our practices meet or exceed consumer expectations and contributing to industry and policy initiatives that enable other companies to do the same.

P&G's approach to privacy is guided by two fundamental principles:

- (1) We strive to treat information provided by individuals as their own, which has been entrusted to us; and
- (2) We strive for transparency with consumers about how their information is used. We inform people about how we handle information they provide us and give them choices about further communication with us and further use of the data.

Our privacy policy is global and we extend the same high level of protection to information from all individuals who provide personal information to us (consumers, shareholders, employees, job applicants, etc), to all locations where we do business and to all channels of contact, such as the Internet, direct mail, telephone, and wireless.

EPC does not contain or collect personal information, nor is it intended to. But there is a perception that the technology could be used in this way. That is why we are working so hard to educate consumers about the facts versus the myths surrounding EPC.

Based on extensive consumer research undertaken on EPC and our own core mission that "the consumer is boss," we worked with our EPCglobal partners to craft usage guidelines for item level EPC in the fall of 2003. To complement these guidelines, P&G's internal position, based on the pillars of fair information practices, are as follows:

- (1) **Clear and accurate notice** should be provided where EPC is being used and consumers should be informed as to whether products they are buying contain EPC tags;
- (2) **Consumers should have a choice** as to whether EPC tags in the products that they buy can be permanently disabled or discarded, and this should be done without incurring cost or penalty;
- (3) **Consumers should have a choice** as to whether personally identifiable information about themselves is electronically linked to the EPC number on products they buy beyond what is done with barcodes today.

Consumers will make choices based on benefits they perceive from the technology. We are working aggressively to identify and communicate these benefits as well as to identify options to implement these principles together with our partners in the supply chain. We will not pursue item-level tagging with partners who are not able to ensure privacy protection for consumers. We serve consumers. To do otherwise would not meet our core mission or business objectives.

In this phase of testing and learning about EPC in 2004, P&G is informing our consumers about the pilot tests we are conducting. Up-to-date information about current tests, locations, brands and type of test (whether pallet/case or case/item) can be found on the company website, www.pg.com. In any pilot where a consumer could come in contact with an EPC tag, P&G affixes a label to the case that notifies the consumer of the presence of a tag. In addition, some retail outlets are providing further information on EPC to consumers in the form of a tear-off card on the store shelf that explains EPC, the symbol, and how the tag can be removed from the carton, and directs consumers to www.EPCglobalinc.org for more information.

NEED FOR CONSUMER EDUCATION

Consumer research shows a very low awareness and understanding level of EPC at this time. P&G along with other end users in EPCglobal recognize the importance of education in gaining consumers' trust in the technology and their understanding of the benefits. Last month we participated in the Federal Trade Commission's workshop on RFID. FTC has played an important role in educating consumers on issues such as safe Internet surfing, online shopping tips, and protecting consumers against ID theft. We are enthusiastic about the potential for FTC to contribute to consumer education and outreach on RFID.

EPC IS IN THE EARLY STAGES OF DEVELOPMENT

In summary, I want to emphasize that EPC is in the early stages of development. The success of EPC depends on collaboration, global standards and affordable technology. We need the ongoing support and involvement of retailers, manufacturers and other industry bodies to adopt the EPC system. EPC must become the single global standard in order for the full efficiencies of the technology to be realized.

Standards enable cost effective, interoperable technology. And finally EPC technology needs to be affordable. The cost of tags and readers must continue to decline in order to deliver a value proposition at the case and pallet level. Item level tagging for consumer products requires tags to cost one cent or less, a threshold that is some years away.

EPC is designed to benefit the consumer. It will help ensure that the right product is in the right place, at the right time and at the right price. In order for EPC to be successful, it must be accepted by consumers, be perceived as offering consumers benefit and be used in ways that provide privacy protection for consumers. Procter & Gamble is working hard to ensure that EPC will be a "win/win" for all.

Thank you for the opportunity to appear before the Subcommittee. I will be happy to answer the Subcommittee's questions.

STATEMENT OF PAULA J. BRUENING

Ms. BRUENING. Mr. Chairman, members of the subcommittee, thank you for the opportunity to speak with you today about the privacy implications of Radio Frequency Identification technology. My name is Paula Bruening and I am Staff Counsel for the Center for Democracy and Technology, a nonprofit, public interest organization that advocates for civil liberties in the digital age.

RFID promises to offer consumers benefits ranging from enhanced drug safety to better security to lower costs through streamlined inventory and delivery systems. We join others here today in looking forward to the realization of that promise. At the same time, the power of RFID and the infrastructure necessary to make the technology work also poses privacy issues that must be resolved if it is to be accepted by consumers.

First, RFID introduces a new method of information collection and sharing in an environment that is already rich with the collection, retention and sharing of personal information. But unlike the information collection technologies with which we've become familiar, the internet, the customer loyalty cards or barcodes, RFID tags are invisible. Inserted into the sleeve of a blouse or the hem of a pair of trousers, consumers may not know at all that these items are being used.

RFID also enables the collection of information without the active engagement of the consumer. When I used a credit card, I am actively deciding to turn over certain information that will make it possible to complete a transaction. I receive a bill at the end of the month reminding me of the details of that transaction. RFID data collection is passive with respect to the consumer. It does not actively engage the consumer at all and provides the consumer with no record that the data collection ever happened. The kind of information potentially collected using RFID is also unique. While we've become somewhat accustomed to the concept of personal profiles that are based on our buying habits, travel activities and demographics, RFID potentially allows much more fine grained data collection than previously possible.

RFID tags can contain globally unique identifiers that distinguish, for example, this particular bottle of Crystal Geyser water from all the other bottles of here at the table or for that matter throughout the world.

When that globally unique ID is linked to the information that uniquely identifies me as a consumer, a company will be able to know, with specificity, not only that I bought a copy of the novel, the Rule of Four, but will know which specific copy of the novel be-

longs to me. As RFID sensors proliferate, the abundance of data collection points also increases, making it possible to track my movements with the book.

Second, in spite of the unique character of RFID technology and data collection, the emergence of RFID and the privacy concern it raises presents yet another example of the need for baseline technology-neutral privacy legislation, based on well-established principles of fair information practices that would clearly delineate the responsibilities of businesses that deploy technologies to collect personal information. Despite on-going public concern about privacy and despite the fact that privacy issues arise with each new technology that collects personally identifiable information, the United States still lacks baseline privacy legislation that would address privacy concerns raised by the collection of this information.

Enactment of this kind of law would not only be an important step in addressing privacy in RFID, but it would also provide the basis for implementation in a privacy respectful way of the next emerging technology.

CDT joins other consumer and privacy advocates also in calling for a full scale technology assessment of RFID. Such an assessment would provide accurate and timely information as well as in-depth neutral analysis that would establish a sound foundation for making policy decisions about the technology.

Finally, the Federal Government has taken a leadership role in adopting and deploying RFID technology to cut down on fraud and waste. While these efforts are laudable and needed, little or no emphasis has been placed on the privacy concerns attendant to the implementation of this technology. The concerns are particularly acute in government implementation of RFID as the technology will likely be tied to services that individuals have no option to receive elsewhere.

CDT calls upon government agencies seeking to deploy RFID to develop privacy guidance for agency use of the technology as they have in the case of electronic authentication. Congress should also explore whether current privacy laws that apply to government collection of information adequately cover the use of RFID by government agencies.

I thank the subcommittee for allowing me to be here today and of course, I'll be happy to answer any questions.

[The prepared statement of Paula J. Bruening follows:]

PREPARED STATEMENT OF PAULA J. BRUENING, STAFF COUNSEL, THE CENTER FOR
DEMOCRACY & TECHNOLOGY

Mr. Chairman and members of the Subcommittee, the Center for Democracy & Technology (CDT) is pleased to have this opportunity to speak to you about both the promise and the possible privacy risks of radio frequency identification (RFID) technology.

CDT is a non-profit, public interest organization dedicated to preserving and promoting democratic values in the digital age. A core CDT goal is to enhance privacy protections for individuals in the development and use of new technologies. We have long advocated the view that privacy considerations are best addressed early in the technology development process, and we applaud the Subcommittee for holding early hearings on this nascent, but potentially revolutionary, technology.

Creative applications of radio frequency identification (RFID) devices hold possibilities for consumers, businesses and government. They can reduce costs in inventory management, improve drug safety, help to reduce error rates and save lives in

hospitals, and better track luggage and cargo at airports to increase homeland security.

There are many possible applications of RFID that do not pose major privacy concerns. But to the extent that RFID devices can be linked to personally identifiable information, RFID raises important privacy questions. In an era of widespread collection of data about individuals, RFID heightens concerns about the ability of businesses and government using these technologies to create deep, rich profiles about people and their travels, lifestyles, interests and activities.

In our testimony today, we wish to emphasize six principle points:

- RFID technology poses significant and novel privacy concerns.
- At the same time, well-established principles of fair information practice provide a ready framework to address many of these issues.
- The privacy concerns raised by RFID can be addressed, but they must be handled early. This will require the engagement and commitment of the companies involved. Good work is already being done, but privacy guidelines for RFID must be specific and clear.
- The privacy concerns with the federal government's use of RFID need considerably more attention.
- Technology-neutral baseline privacy legislation could answer many of the basic concerns posed by RFID without creating technology mandates. Legislation aimed specifically at RFID technology is probably undesirable. Companies should not be deploying RFID devices in situations that involve correlation of personally identifiable information until the rules are clear.
- A comprehensive technology assessment is needed at this time. Such an assessment would provide critical information that would help lawmakers, privacy and consumer advocates, technology developers and businesses to avoid serious potential pitfalls.

1. NOVEL PRIVACY ISSUES RAISED BY RFID

Discount cards, other "customer loyalty cards" and credit cards already collect information about individuals, providing a rich store of information about our likes and dislikes in cars, clothing, travel and many other preferences. The extent to which RFID tags possess the ability to further enhance those profiles by tracking an individual's movements—whether through a store or through the world—will raise new and deeper concerns. The freedom to move freely and without being monitored is basic to the American concept of individual autonomy.

These concerns are further heightened as the wall between government and business collection of information becomes increasingly porous, and as government looks increasingly to commercial databases as a resource for homeland security and law enforcement.

Information gathering using RFID differs from other kinds of data collection in at least three significant ways:

- First, it is **invisible** to consumers: unless the consumer is made aware of the technology, he or she will likely not know that the devices are in use. Data collection occurring with a loyalty card or a bar code involves a visible device that the user can see and touch when the collection takes place. RFID raises the specter of data collection via a device of which the consumer may not even be aware in the sleeve of a blouse or the hem of a pair of trousers.
- Second, the information collection is **passive** with respect to the consumer. A consumer using a credit card actively relinquishes either the card or the account number to a business to make payment for goods or services. In the act of giving the credit card or number, the consumer actively decides to engage in a system that collects certain information about the transaction, not only about the account, but also about the nature of the goods purchased, and when and where the transaction occurred. The consumer is reminded of the event when he receives a statement at the end of the month that specifies when the card was used and what charges were incurred. In contrast, information can be collected by RFID absent any active step on the part of the consumer to turn over the information, and no record of the collection is provided to the consumer.
- The **kind of information** potentially collected using RFID is unique. While we have become somewhat accustomed to the concept of personal profiles that are built on our buying habits, travel activities and demographics, RFID potentially allows much more fine-grained data collection than previously possible. RFID tags can contain globally unique IDs that distinguish a particular book from all other copies of that book. As RFID sensors proliferate, the abundance of collection points—and the detail of location data that can be gathered—also increases.

Together, these changes enable data collection and sharing scenarios that are currently impossible. For example, today, the use of “frequent buyer” cards (also known as “customer loyalty cards”) allow stores to keep records of consumer purchases over time, even when payments are made with cash. With RFID, however, it is possible to track not just what items consumers leave the store with, but also where they go with such items and for how long they keep them. If RFID were built into consumer “loyalty cards” it would also be possible to tell not only what you bought but also what you looked at. RFID transfers to the brick and mortar world the type of very specific tracking of interests that is possible online. Without notice, consumers would not necessarily be aware that this kind of tracking was going on.

Similarly, the proliferation of RFID technology raises heightened concerns about data sharing and centralization. There is a strong analogy in this case with our experience with “cookies.” While cookies were originally designed to allow consumers to have a consistent experience within a single website, the spread of the technology eventually gave rise to information from across websites being linked through third-party cookie systems. Similar problems could arise with RFID, because an RFID reader can typically read any tag. As readers proliferate in stores, libraries, hospitals, and public places, there will be strong incentives for companies to share and link information about the tags they distribute and the tags they read.

The comments of technologists at recent events sponsored by the National Academy of Sciences and Department of Commerce indicate that while the power of this technology is currently limited, developers are working to increase the amount of information the tags can hold, enhance the effectiveness of the readers, lower the cost of the technology, and make the infrastructure far more ubiquitous.

2. FAIR INFORMATION PRACTICES

RFID implementation must be guided by principles of fair information practice that give consumers control over the collection and use of their personal information.

In 1973, at the beginning of the computer revolution, principles of fair information practices were articulated as guidelines for protecting privacy. These principles form the basis of the Privacy Act of 1974 and similar laws enacted at the state level. They also serve as the foundation of laws enacted at the federal level to address privacy in specific sectors, notably in credit, medical, and financial records. They have been incorporated into industry codes of best practices and form the underpinnings of international agreements on data protection. The principles are intended to give individuals control over their personal information, limit data collection, and place responsibilities on data collectors.

While exact formulations of fair information practices differ, the common elements are relatively standard. They include:

- *Notice*: Information collection and use should be open and transparent.
- *Purpose specification*: Personal data should be relevant to the purposes for which it is collected.
- *Use limitation*: Data should be used only for the purpose for which it was collected.
- *Accuracy*: Personal data should be accurate, complete, and timely.
- *Security*: Personal data should be protected by reasonable security safeguards against risk of loss, unauthorized access, destruction, use, modification or disclosure.
- *Access*: Individuals should have a right to view all information that is collected about them to correct data that is not timely, accurate, relevant or complete.
- *Accountability*: Record keepers should be accountable for complying with fair information practices.

In November of last year, CDT joined with a broad coalition of privacy and civil liberties organizations in calling for the application of fair information practices to RFID.¹ These principles should apply to the gathering of information using RFID and to the handling of that information. They provide a starting point for all ongoing and future efforts to understand and address the RFID privacy issue.

Determining how fair information practices can be applied in a practical, useful and meaningful way will require work on the part of stakeholders.

¹ The “Position Statement on the Use of RFID on Consumer Products” November 14, 2003 was issued by: Consumers Against Supermarket Privacy Invasion and Numbering (CASPIAN), Privacy Rights Clearinghouse, American Civil Liberties Union (ACLU), Electronic Frontier Foundation (EFF), Electronic Privacy Information Center (EPIC), Junkbusters, Meyda Online, PrivacyActivism and endorsed by many others including CDT. It is available at <http://www.privacyrights.org/ar/RFIDposition.htm>.

3. ADDRESSING PRIVACY AT THE OUTSET: INDUSTRY ENGAGEMENT AND BEST PRACTICES

If companies and government are to successfully and responsibly deploy RFID technology, they need to address upfront the significant trust issues the technology raises. Using RFID in pallets to assist distribution processes and inventory control does not raise major privacy concerns. But as soon as RFID tags are related directly to individual product items, it will be extremely important that consumers clearly understand that the technology is in use, what information is being collected, how it is collected, and how it is used. If consumers are to accept the use of this technology, it is critical that they have assurances that information collected through RFID is managed and used in a responsible fashion.

Experience has shown that when new information collection technologies are deployed, consumers want to know specifics about what and how data about them is being gathered. They want to know upfront from the organization collecting the information, and not through the popular media. It is critical with RFID, as in other emerging technology, that privacy protections are built in at the beginning.

Technology developers and businesses often raise the issue of the cost of building privacy into new technology. CDT would caution that **it is more effective and efficient to begin at the outset of the development process to create a culture of privacy that incorporates sound technical protections for privacy and that establishes the key business and public policy decisions for respecting privacy in RFID use before RFID is deployed, rather than building in privacy after a scandal or controversy erupts publicly.**

Work toward developing principles that would address privacy concerns raised by RFID is ongoing. For example, CDT applauds EPC Global for their work on public policy guidelines that address privacy issues.² However, for these principles to be successful in protecting privacy, it is critically important to concretely determine how these principles are applied in practice.

For example, notice and public education are often pointed to as key to sound privacy protection for RFID data collection. This is undoubtedly true. But while we may easily agree on this point, it will be extremely important to understand how notice can be *effectively* provided in the RFID environment, in a manner that is consistent and balanced, where information collection is arguably invisible and passive. How to provide notice effectively, and in a manner that is consistent for consumers and presented in a balanced, neutral way, will be a critical challenge.

Similar issues are raised as steps are taken to provide consumers with choice about collection of information through RFID. How do we provide meaningful choice for consumers? How do we make it easily accessible and exercisable in this kind of technology environment? How can we assure that consumer choice has been respected?

4. GOVERNMENT USE OF RFID RAISES SPECIAL CONCERNS AND REQUIRES SPECIAL CONSIDERATION

Federal, state and local governments have taken a leadership role in the deployment and use of RFID technology. Some governments have used the launch of RFID applications as an opportunity to balance privacy concerns with the use of the technology. For example, the Office of the Information and Privacy Commission of Ontario has released "Guidelines for Using RFID Tags in Ontario Public Libraries."³ U.S. governments have undertaken little of this important work.

The Department of Defense has been a leader in the RFID field and is engaging in innovative uses of the technology for tracking items within its warehouses.⁴ Other federal agencies are following suit with projects outside of the warehouse, such as the Department of Homeland Security's enormous US-VISIT contract.⁵ While the government should be encouraged to develop uses of RFID technologies to increase efficiency and cut down on fraud and waste, little or no emphasis has been placed on the privacy concerns attendant to the deployment of the technology. The concerns are particularly acute in government implementation of RFID, as the technology will likely be tied to services that individuals have no option to receive elsewhere.

²"Guideline on EPC for Consumer Products" is available at http://www.epcglobalinc.org/public_policy/public_policy_guidelines.html.

³<http://www.ipc.on.ca/docs/rfid-lib.pdf>

⁴Andrew T. Gilles, "Pentagon: Rough RFID Ride Ahead," *Forbes.com*, July, 7, 2004, http://www.forbes.com/technology/enterprisetech/2004/07/07/cz_ag_0707beltway.html

⁵Jonathan Krim, "U.S. May Use New ID Cards At Borders," *Washington Post*, June 5, 2004, page E1.

CDT calls upon the Office of Management and Budget (OMB), General Services Administration (GSA) and National Institute of Standards and Technology (NIST) to develop privacy guidance for agency use of RFID, as they have for electronic authentication technologies. Congress should also explore whether current privacy laws, such as the Privacy Act, Computer Matching and Privacy Protection Act and Section 208 of the E-Government Act, whether these laws adequately cover use of RFID by government agencies.

5. BASELINE PRIVACY LEGISLATION WOULD ADDRESS MANY OF THE ISSUES POSED BY RFID

Despite ongoing public concern about privacy, and despite the fact that privacy issues arise with each new technology that collects personally identifiable information (e.g., cookies, spyware), the United States still lacks baseline privacy legislation that would address privacy concerns raised by the collection of personally identifiable information in new digital media.⁶

In our view, in the absence of such legislation and in the absence of clear, specific industry guidelines, it is unwise for companies to deploy RFID technologies in consumer applications that involve personally identifiable information. Implementing RFID without this guidance raises the risk that it will be necessary to impose rules after the technology has been deployed, when rules may be more cumbersome and less effective, and when it is less likely that technical protections for privacy can be optimally integrated into the technology. It is for this reason that CDT and others have said that RFID should not be deployed at the consumer level in ways that can be linked to personally identifiable information until privacy guidelines are put in place, either by industry, the Congress or state legislators.

CDT believes that it would not be appropriate to enact legislation specially regulating RFID. To enact legislation specifically for RFID would risk technology mandates that are ill-suited to the future evolution of the technology. On the other hand, technology-neutral baseline privacy legislation would ensure that retail and marketing uses of the technology in conjunction with personal information were bounded by fair information practices. Location information, whether generated by cell phones, by mobile computing, or by RFID, also merits stronger privacy protections.⁷ These two crucial privacy issues should be addressed in technology-neutral ways.

6. THE NEED FOR TECHNOLOGY ASSESSMENT

While specific regulation of RFID technology may be inappropriate, a technology assessment conducted by an expert panel is sorely needed. Such an assessment could be conducted under the auspices of the National Academy of Science, the Federal Trade Commission (FTC), or the National Institute of Standards and Technology (NIST).

Already legislatures are beginning to look at RFID and the privacy concerns the technology raises. Both industry and consumer groups are developing privacy guidelines for use of the technology. But stakeholders on all sides of the debate share a concern about institutionalizing solutions that stifle innovation and have unintended and unwanted consequences for privacy and for RFID technology. Any decision about privacy must be based on sound analysis, the input of all stakeholders, reliable information, and a clear understanding of the technology—both its potential benefits and the risks it raises.

CDT believes that a technology assessment could provide critical information that would help legislators, policy experts, technology developers and businesses to avoid these pitfalls. Technology assessment—an analysis of RFID that explores the technology, how it works, its potential to serve individuals, the vision for the future of the technology, how its use may proliferate and develop and the risks it raises for privacy—could provide the analytical underpinnings to make possible the best possible resolution of privacy concerns. Technology assessment could also surface concerns that are not immediate but that are raised through the establishment of an infrastructure for RFID.

⁶See the testimony of CDT President Jerry Berman before the full Senate Commerce Committee on October 3, 2000 at <http://www.cdt.org/testimony/001003berman.shtml>. His testimony addressed S. 2606, a bill that passed the Committee that year and would have created a baseline standard for privacy on the Internet and allowed the FTC to create regulations for offline privacy in the retail and marketing space.

⁷See the testimony of CDT Executive Director James Dempsey before the Subcommittee on the Constitution of the House Judiciary Committee on September 6, 2000 at <http://www.cdt.org/testimony/000906dempsey2.shtml>. His testimony addresses H.R. 5018, a bill that passed the Committee that year and would have increased location standards for the use of information by law enforcement.

Such an assessment would bring to bear the expertise of technologists, academics, privacy advocates, consumer advocates, manufacturers, retailers, security experts and other potential users of RFID technologies. Many of these efforts are already ongoing in public interest organizations and in business research, so that many of the individual pieces of a technology assessment are already in progress. A formal technology assessment would capitalize on these efforts, draw this work together and provide neutral, balanced analysis.

It is important to note that when done well, technology assessment does not arrive at facile solutions. When done fairly, it does not yield simple answers to satisfy a single interest group. Rather, it provides policy options based on the richest, most accurate store of information about the issue possible and the most balanced analysis available. Timeliness is, of course, always a concern when developing technologies are at issue. The online tools at our disposal should make it possible to engage in the assessment exercise in a timely manner that serves both the needs of business for prompt input and the needs of all stakeholders for a chance to bring their concerns to the discussion.

Conclusion
CDT urges Congress to continue to closely monitor the privacy concerns raised by RFID. Business, technologists and consumer advocates must continue to address this issue as the technology and its applications are developed. Additional Congressional hearings would reinforce the need for ongoing work in the private sector to develop and institute best practices for privacy in RFID use. Baseline privacy legislation would help address significant privacy concerns raised by RFID, as well as by other developing technologies. While it is possibly unwise to create RFID specific regulation at this time, we urge Congress to request that the National Academy of Sciences or another neutral, expert body conduct a technology assessment that would provide the technical and policy underpinnings for the best possible legislative solution, when it is timely and appropriate. We look forward to working with the Committee on this critical issue.

Mr. STEARNS. I thank the gentlelady.

Mr. Galione.

STATEMENT OF WILLIAM GALIONE

Mr. GALIONE. Mr. Chairman, members of the committee, I thank you for the opportunity to testify on behalf of Philips Semiconductors on the very important subject of Radio Frequency Identification technology. In my brief comments this morning, I'd like to focus on from the perspective of the leading semiconductor designer and manufacturer of RFID products, basically what it is and where it's used.

Just for some context, Philips Semiconductors is a division of Royal Philips, so we're a \$5 billion division of the \$35 billion that is Royal Philips. Philips is a large consumer electronics, lifestyle, healthcare and technology company. We're the semiconductor arm with more than 100 sales offices. We operate in 50 countries, many, many manufacturing locations around the world. But to amplify the point that this is not a new technology, Philips Semiconductors has shipped more than one billion contactless ICs in the history of that product portfolio, so it's been around for a while, commercialized over the past 15 to 20 years, but it's been around as was stated previously for many, many years.

Basically, there are two types of identification products. The first one is contactless smart cards, things like this, credit card size things. The key to these and I'll pass these around later to members of the committee, if you'd like it, the key is that this securely identifies people, to grant people access to services so therefore very short range, three to four inches away from the reader. But the key is that it is secure information about people. RFID tag, on the other hand, these tags and labels, again, I'll pass these around

if you'd like them, are for to track and trace goods, much longer range vicinity, 10 to 20 feet as was stated previously.

So again, in terms of the contact with smart card technology, it's a card form factor, a combination of security and convenience, short operating distance, but very, very secure and it can be for moderate to strong security, but the strongest security involves some very advanced encryption technologies and algorithms, password protection and mutual authentication between the card and the reader. The cost of these things, because they are fairly sophisticated, semiconductor designs, would be between \$1 and \$20. The kinds of applications that they find their way into are public transportation, more than 200 cities around the world are currently using these. Five hundred million cards are deployed around the world. Payment, companies like Visa, Mastercard, American Express and of course loyalty programs, access controls, so you can get into a building, car and mobilization is an emerging application for these, event ticketing and identification of individuals and evolving into, in fact, passports in the future.

The RFID technology, again, the tags and labels here, it's—that's the form factor of it. Carries a unique identification number as previously said, plus optional read/write memory, can communicate to the tag, not just have information from the tag, low to moderate security features because it is goods, not people, but does have a unique destroy feature, so as we evolve into the item world at the option of the consumer, it can be destroyed, rendered totally disabled once you would leave the store and then the operating distance, as I said previously, is about 20 feet. Very low cost, going from just a few cents, in fact, to a couple of dollars, depending on application and the key applications are identifying and tracking goods and logistics, kinds of applications, supply chain management, manufacturing and warehouse automation, parcel services. We'll see that evolving into baggage tagging and tracking and tracing. Asset management, we're seeing applications in library automation, livestock management and in fact, things like in the future even laundry automation so your red socks don't get combined with your white shirt when you have a smart washing machine.

So overall, those are the applications. That's the perspective from the way we see it as a semiconductor maker. We're aware of the privacy concerns raised by consumers over the use of this technology and are working very closely with privacy organizations and government officials around the world to ensure a responsible roll out of RFID and we look forward to assisting the committee in any way that you see appropriate in the future.

[The prepared statement of William Galione follows:]

PREPARED STATEMENT OF WILLIAM GALIONE, VICE PRESIDENT AND GENERAL
MANAGER, MARKETING AND SALES AMERICAS, PHILIPS SEMICONDUCTORS

Mr. Chairman, thank you for this opportunity to testify on behalf of Philips Semiconductors on Radio Frequency Identification (RFID) technology. Philips Semiconductors is a product division of Philips Electronics, well-known throughout the world for its innovative consumer electronics, lifestyle and healthcare products. Philips is the world's leader in the design and manufacturing of contactless identification chips, with nearly one billion chips sold to date. Philips' contactless identification technology is used across a diverse set of applications—such as supply chain management and logistics functions, including pharmaceutical and livestock track-

ing, as well as in various transport, banking and security applications—to provide consumers with greater convenience and safety.

Philips offers its contactless identification technology as an open platform and is an active promoter of global standards to build the foundation for widespread adoption. With new applications in the consumer retail market on the horizon, Philips has built a complete catalog of contactless chip technology that spans the application range of tags, contactless smart cards, car immobilizers, and the corresponding reader components.

I'd like to provide a brief overview of the two most common applications of contactless identification technology: identifying goods and granting people access to services. The term "RFID" is broadly used to describe a "smart tag" or "smart label" or simply "RFID tag" used to identify goods or products. You may also have heard the term "smart card," which is essentially a personal RFID device used by people to identify themselves, for example, when entering a building or using the Washington, D.C. Metro system. Simply put, a smart card carries a secure chip with advanced encryption, computing power and a contactless RF—interface that provides consumers with a high degree of functionality with enhanced personal privacy and security.

CONTACTLESS IDENTIFICATION TECHNOLOGY AND GOODS

Almost every item sold through retailers and supermarkets around the world today has a barcode printed on it. These codes are used extensively throughout distribution chains and are unique to the general type of item being sold. However, in recent years barcodes have begun to show their limitations, and a replacement approach based on RFID technology is gaining momentum.

RFID technology relies on small computer chips and antennas integrated into a paper or plastic label—called a tag—that can be scanned by an electronic reading device. The scan allows automatic collection of data on the chip, which can include information on warranty, where the product was manufactured, or product details such as quantity, size, color, etc. First developed in the 1940's, RFID technology has proven itself reliable over time, with falling cost structures and further technology refinement allowing it to be used in more common applications today.

Unlike barcodes, RFID tags are insensitive to dirt or scratches and can be scanned from a distance—from a few inches to upwards of 20-25 feet—all without requiring direct line of sight. RFID technology also allows multiple tags to be scanned simultaneously, even through external packaging. This presents a significant advantage over barcodes in distribution and retail environments, which is where the new generation of RFID technology is making major inroads.

Adoption of RFID technologies is spearheading revolutionary gains in supply chain management, allowing businesses to improve supply chain logistics and customer service. Major retailers—including co-panelist Wal-Mart and other organizations such as the Department of Defense—that manage huge inventories are leading the supply chain transition to RFID technology.

The Wireless Data Research Group predicts that the RFID market for hardware, software, and services is expected to increase by a 23 percent compound annual growth rate worldwide from more than \$1 billion in 2003 to about \$3 billion in 2007. According to analyst firm IDC, RFID spending for the U.S. retail supply chain will grow from \$91.5 million in 2003 to nearly \$1.3 billion in 2008. This increase is due in large part to the mandates by leading retailers and the U.S. government to incorporate the technology, and also to increasing RFID adoption in many other application areas.

A recent report by AMR Research on the supply chain results achieved by early adopters of RFID technology in the retail and consumer packaged goods arena showed cost savings of 5 percent of sales. This included savings of 1 percent of sales due to reductions in product loss. The retailers also reduced their expenses by 65 percent in the receipt of goods arena and 25 percent in stocking.

RFID tracking of pallets and shipping cases—from the manufacturer, to the warehouse, to the distribution center, to the final destination—is expected to deliver increased efficiency, more timely and accurate management of inventory, greater responsiveness to product recalls, and reductions in theft and counterfeit goods entering the retail arena. Pharmaceutical companies are also planning to use RFID systems to ensure the quality of their goods. Recent headlines about the need for live-stock tracking reports related to disease prevention underscore the need for accurate real time information, which RFID can provide.

In addition to the consumer applications cited earlier, RFID tags are also being considered for item-level identification of goods purchased by consumers once the cost structure is low enough. Many item-level identification benefits can be found

in the retail environment following successful implementation within a supply chain. Retailers will be able to pass on the savings to their customers and also provide consumers with greater convenience, value, choice, and protection. Co-panelists Wal-Mart and Procter and Gamble can provide more information on plans for item-level identification.

CONTACTLESS IDENTIFICATION TECHNOLOGY AND PEOPLE

Contactless identification technology is also used for personal identification, including in so-called "smart cards." Smart cards typically come in a credit card form factor and carry sensitive, personally identifiable data. American consumers are likely to encounter smart cards and similar RF-enabled personal identification devices in their daily lives through applications such as secure access cards for building entry, speedy gasoline purchasing such as the Exxon Speedpass, vehicle anti-theft systems, and in transportation systems all over the world, including in the Minneapolis, San Francisco, Seattle, San Diego (in Subcommittee member Congressman Issa's district), Houston, and other systems.

Smart cards are essentially RFID systems with advanced computing power, storage, and strong encryption accelerators, offering advanced services with enhanced security and privacy protection.

In fact, smart cards are so powerful that the Department of Defense (DoD) and other government agencies are adopting the technology to secure access to their facilities and computer networks, even storing a picture and fingerprint of the cardholder on the card for enhanced security control. The DoD makes worst case scenario assumptions about the cards falling into the wrong hands and having large resources at their disposal to crack the card—standards that advanced smart cards have met through the use of encryption, secure design, and other measures.

The United States and leading countries all over the world are presently working on the specification and deployment of contactless smart card technology for the use in passports. Like the DoD's Common Access Card, these passports will carry biometric credentials such as fingerprints, pictures and/ or iris-scans to securely identify and authenticate the passport holder.

PRIVACY

Philips is aware of some of the privacy concerns raised by consumers over the use of RFID technology. For consumers, for whom item-level identification benefits are perhaps several years away, there has already been concern expressed regarding the ways in which the information on the tag will be used. Manufacturers have responded with a feature that can destroy the tag at checkout, and have increasingly recognized the need for education on the technical capabilities of the technology and privacy implications. This includes communicating the safeguards built in to the chips to protect against unauthorized scanning and tampering, as well as explaining how the limits of the technology prevent such impossible scenarios as satellite tracking of an RFID-tagged item.

Philips is working with privacy organizations and government officials to ensure a responsible rollout of RFID in the retail environment. Philips Semiconductors co-hosted with the National Retail Federation a well-attended RFID privacy roundtable in Washington, D.C. on April 27, featuring industry, privacy advocates, and state legislative officials discussing privacy issues and RFID technology. Last year, Philips presented its views on privacy issues of RFID technology to the 25th International Conference of Data Protection and Privacy Commissioners in Sydney, Australia and fully supports the Conference's resolution on RFID and privacy. When the MIT hosted an RFID Privacy Workshop in November 2003, Philips presented the 101 of RFID Technology and its Applications. Philips also participated in the recent Smart Tags Workshop of the European Commission in Brussels, where it renewed its offer to help (privacy) authorities understand RFID-technology. Most recently, Philips served as a panelist in a RFID workshop hosted by the Federal Trade Commission, offering an overview of the technology.

CONCLUSION

Mr. Chairman, thank you again for this opportunity to provide an overview of contactless identification technologies to the Committee. As the world's leader in the design and manufacturing of chips used in contactless smart cards and RFID tags, Philips is committed to the responsible rollout of RFID technology across a wide spectrum of retail and personal identification applications, and stands ready to provide you with any assistance you may need as the US Congress further studies this revolutionary technology.

Mr. STEARNS. I think the gentleman, Mr. Galione.
Mr. Steinhardt.

STATEMENT OF BARRY STEINHARDT

Mr. STEINHARDT. Thank you, Mr. Stearns and members of the committee, for the invitation to testify today.

My testimony this morning is going to focus on the government use of RFID. In my written testimony I also address the use by the private sector.

RFID chips can be used for good or ill, as you've heard so far. But their attributes are worth focusing on for a moment.

First, as already indicated, the chips—

Mr. STEARNS. I'm going to have you pull the mic, bring it down and just closer to you.

Mr. STEINHARDT. Is that better?

Mr. STEARNS. Yes, that's better.

Mr. STEINHARDT. The chips can track not just goods, but people. Chips emit a signal which enables a remote, even surreptitious identification. You had a demonstration of that this morning.

Many deployments of RFID will require the creation and use of data bases containing personal, sometimes sensitive personal information. RFID use is easily integrated into those data bases and with other technologies.

The government use of RFID is virtually—I apologize, it's cutting of here.

Mr. STEARNS. That's okay.

Mr. STEINHARDT. The government use of RFID is burgeoning. The Pentagon, for example, plans to use RFID to track physical objects, the use that raises relatively modest privacy concerns. Other proposed uses raise more serious concerns. The San Francisco Library would like to put RFID chips in its books, raising the specter of third parties being able to track our reading choices.

More troubling are proposals to put RFID chips into government-issued identity documents. The example which has perhaps the most profound implications and has largely gone unnoticed by the press and many public policymakers that's been alluded to here this morning is that at the urging of the United States government, indeed, the instruction of the Congress as part of the Border Security Bill. The International Civil Aviation Organization, ICAO, which is U.N.-affiliated agency has been developing the global standards for passports and other travel documents. ICAO's current proposal which developed a process in which the public was excluded, and indeed in my written testimony I detail our futile attempts to even engage ICAO in a discussion, but their current proposal is a passport that is laden, not only with biometrics like a finger scan or a digital photograph, but with RFID chip or what ICAO calls a "remotely readable contact-less integrated circuit", but in fact, they mean RFID chip.

ICAO proposes to create a whole new class of identity document that could be used to identify us anywhere, any time. Like most processes with limited input, the standards developed by ICAO are equally flawed. The RFID chips under consideration can be read from up to a meter away, roughly three feet and have enough

memory to hold full biometric information such as fingerprints and photographs.

The potential uses and abuses of such a chip raise profound questions. Imagine, for example, the uses that could be put to by a dictator like Fidel Castro. Every Cuban citizen, indeed, every American traveling to Cuba, perhaps to visit a relative would be under a new and powerful surveillance regime.

And the misuse is not likely to be limited to dictatorial regimes. RFIDs would allow for convenient at a distance identification. RFID tag IDs could be secretly read through a wallet, pocket, backpack or purse by anyone, an inappropriate reader, including marketers, identity thieves and pickpockets.

Pocket ID readers could be used by government agencies to sweep up the identities of everyone at a political meeting, protest march or religious service. A network of automated RFID listening posts on the sidewalks and the roads could even reveal the location of people using those sidewalks and roads.

Now indeed, there are two possible paths by which RFID powered-passports could become tools for tracking the every day lives of Americans. First is in passports that are being developed by ICAO, could be seen as the gold standard of identity verification around the world. More and more, as they are demanding proof of identity, not only abroad, but within the United States, they could displace driver's licenses, primarily form of identification in every day life. Or those ICAO passports could become a template for standardized versions of the driver's license, turning them into a de facto national ID card, but in effect, a super charged national ID card.

Congress needs to focus attention on its development and have a serious debate about how and when Americans will be identified and tracked both here and around the world. At the outset, Congress will need to decide whether we're willing to go down this path incorporating RFID into our identity documents or choose a less invasive technology, like the two-dimensional bar code. We, of course, prefer to choose the latter.

Over the longer term, Congress needs to consider how the fair information principles, some of my fellow panelists have discussed be applied to RFID. This debate needs to be held now before the technology and its uses become a runaway train. If RFID is to be employed, it must be carefully controlled, yet none of these controls currently exist.

Since we regard this debate as so important, we'll be sending copies of my testimony this morning to the other committees of Congress that may have jurisdiction over some of these matters.

The ACLU urges you to be vigilant in monitoring these developments and creating legal controls to protect American privacy, both domestically and internationally.

Thank you.

[The prepared statement of Barry Steinhardt follows:]

PREPARED STATEMENT OF BARRY STEINHARDT, DIRECTOR, TECHNOLOGY AND LIBERTY PROJECT, AMERICAN CIVIL LIBERTIES UNION

My name is Barry Steinhardt and I am the director of the Technology and Liberty Program at the American Civil Liberties Union (ACLU). The ACLU is a nationwide, non-partisan organization with nearly 400,000 members dedicated to protecting the

individual liberties and freedoms guaranteed in the Constitution and laws of the United States. I appreciate the opportunity to testify about Radio Frequency Identification (RFID) tags on behalf of the ACLU before the Commerce, Trade and Consumer Protection Subcommittee of the House of Representatives Committee on Energy and Commerce. Today, I will explore with you the risks to privacy of governmental uses of RFID tags in identification documents, and the risks to consumer privacy of use of RFID tags by the private sector. I will close by suggesting that Congress play an active role in deciding whether to authorize governmental use of RFID tags in U.S. passports.

RFID tags are tiny computer chips connected to miniature antennae that can be placed on or in physical objects. The chips contain enough memory to hold unique identification codes for all manufactured items produced worldwide. When an RFID reader emits a radio signal, nearby tags respond by transmitting their stored data to the reader. With passive RFID tags, which do not contain batteries, read-range can vary from less than an inch to 20-30 feet, while active (self-powered) tags can have a much longer read range.

DRIFT TOWARD A SURVEILLANCE SOCIETY

The privacy issues raised by RFID tags are vitally important because they are representative of a larger trend in the United States: the seemingly inexorable drift toward a surveillance society. As Congress considers the privacy issues posed by RFID chips, I urge you to view them in the larger context—a world that is increasingly becoming a sea of data and databases, where the government and private corporations alike are gathering more and more details about our everyday existence.

The explosion of computers, cameras, sensors, wireless communication, GPS, biometrics, and other technologies in just the last 10 years is feeding what can be described as a surveillance monster that is growing silently in our midst. Scarcely a month goes by in which we don't read about some new high-tech method for invading privacy, from face recognition to implantable microchips, data-mining to DNA chips, and now RFID identity tags. The fact is, there are no longer any technical barriers to the creation of the surveillance society.

While the technological bars are falling away, we should be strengthening the laws and institutions that protect against abuse. Unfortunately, in all too many cases, even as this surveillance monster grows in power, we are weakening the legal chains that keep it from trampling our privacy. We should be responding to intrusive new technologies by building stronger restraints to protect our privacy; instead, all too often we are doing the opposite. (The ACLU has written a report on this subject, entitled *Bigger Monster, Weaker Chains: The Growth of an American Surveillance Society*, which is available on our Web site at www.aclu.org/privacy.)

We hope that this will not happen with RFID chips, which promise great new efficiencies and conveniences, but also hold the potential to enable the most Orwellian kinds of surveillance. RFID tags enable remote, even surreptitious identification; their use generally requires the creation of databases containing identity information; and RFID use is easily integrated into database systems and other technologies.

Congress must act to lay to rest the privacy fears surrounding this technology so that it will be smooth sailing for us all to enjoy its benefits.

There are two primary areas where RFIDs raise privacy issues: their use in retail and elsewhere in the commercial sector, and their direct adoption by government.

THE MOST FRIGHTENING USE OF RFID CHIPS: GOVERNMENT TRACKING

Government use of RFID is burgeoning. The Pentagon plans to use RFID to track physical objects—a use that raises relatively modest privacy concerns. Other proposed uses raise more serious concerns. The San Francisco Library, for example, is proposing to put RFID chips in its books, which raises the specter of third parties being able to track our reading habits without our knowledge.

Most troubling of all are proposals to incorporate RFID tags into government identity documents.

RFIDs would allow for convenient, at-a-distance verification of ID. RFID-tagged IDs could be secretly read right through a wallet, pocket, backpack, or purse by anyone with the appropriate reader device, including marketers, identity thieves, pick-pockets, oppressive governments, and others. Retailers might add RFID readers to find out exactly who is browsing their aisles, gawking at their window displays from the sidewalk—or passing by without looking. Pocket ID readers could be used by government agents to sweep up the identities of everyone at a political meeting, protest march, or Islamic prayer service. A network of automated RFID listening posts

on the sidewalks and roads could even reveal the location of all people in the U.S. at all times.

This may sound far-fetched, and I hope that it stays that way. But if we at the ACLU have learned anything over the past decade, it is that seemingly distant privacy invasions that sound right out of science fiction often become real far faster than anyone has anticipated. I give you this scenario as something that I think most Americans would agree is something that should be avoided, and yet is now entirely possible as far as the technology that is available to us. That means that our future is now going to be decided by *policy*.

RFID-POWERED DOCUMENTS: ALL-TOO REAL

We need not end up in the frightening situation that I have just described to suffer privacy invasions from RFID technology. In fact, worries about RFID-enabled identity documents are far from an abstract concern. Already, deliberations are underway to encourage governments to include RFID chips in the passport carried by citizens of every nation including the United States.

Largely unnoticed by the press and many public policy makers, an obscure UN-affiliated group called the International Civil Aviation Organization (ICAO) has been developing global standards for passports and other travel documents. This effort grows out of the Enhanced Border Security and Visa Entry Reform Act (EBSA), which mandated that the passport of every visa waiver country “issue to its nationals machine-readable passports that are tamper-resistant and incorporate biometric and document authentication identifiers;” any nation that fails to comply with this requirement will lose its status as a “visa-waiver” country.¹ The Act mandates that the standards for these passports be created by ICAO.

Under ICAO’s current proposal, passports around the world would not only incorporate biometrics like fingerprints or face recognition, but—as we only recently learned—also remotely readable “contact-less integrated circuits,” or RFID tags. Nothing in EBSA requires the inclusion of an RFID chip on passports.

While we’ll be making this testimony available to other committees that would have a strong interest in whether RFID tags go on passports, we believe that a wholistic approach to the use of RFID tags by Congress may be called for.

ICAO has been developing these passport standards over a period of months in meetings held around the world. Because of the serious implications of creating an RFID-enabled identity document, the ACLU and the London-based group Privacy International tried to arrange attendance of a representative at a March 2004 meeting held in Cairo. This effort was unsuccessful. An open letter to the ICAO on privacy concerns over the biometric standards likewise met with no response.² The ACLU again wrote to ICAO asking to attend a May 2004 meeting in Montreal, and once again received no response.

In short, despite the importance of technical and interoperability standards—which can mean the difference between a use of biometrics that poses enormous problems for privacy, or one that poses little—ICAO has ignored attempts by privacy and civil liberties groups to join in their process. To a degree that would not be possible with a domestic government decision-making body, it has rebuffed NGO attempts to provide input on the privacy implications of the particular standards being considered, or even simply to observe the meetings.

Like the results of most processes with limited input, the standards developed by the ICAO are deeply flawed. The RFID chips under consideration can be read from up to a meter away and have enough memory to hold full biometric information such as fingerprints or photographs. The potential uses and abuses of such a chip could be revolutionary. A retail store or restaurant, for example, might gain the ability to capture the identities of those who walk through a portal; a government official could instantly sweep the room to discover who is attending a political meeting. Imagine the uses to which a dictator like Fidel Castro could put such technology. Every person in Cuba—including Cuban-Americans carrying U.S. passports while visiting family members in Cuba—could be put under surveillance and no one would be safe.”

If the United States mandates the creation of an international standard for passports, it will face enormous pressure to conform its own passports to that standard. For instance, when the US instituted the US Visit Program one nation, Brazil, reacted swiftly by putting similar measures into effect for just their American visi-

¹ 8 U.S.C. 1732.

² See ACLU et. al., “An Open Letter to the ICAO,” March 30, 2004; online at <http://www.aclu.org/Privacy/Privacy.cfm?ID=15341&c=130>.

tors.³ In fact, far from being concerned that such systems would lead to the retaliatory creation of systems for tracking Americans elsewhere in the world, Bush Administration officials have embraced such reciprocity. “We welcome other countries moving to this kind of system,” Department of Homeland Security undersecretary Asa Hutchinson declared. “We fully expect that other countries will adopt similar procedures.”⁴

By instituting RFID chips in passports, the US government could skip right over the politically untenable proposals for a National ID card, and set a course toward the creation of a *global* identity document—or, at least, toward a set of global standards for identity that can be incorporated into a wide variety of national identity documents. There are two possible paths by which RFID-powered passports could become tools for tracking the everyday lives of Americans:

- These passports come to be seen as the gold standard of identity verification around the world. More and more, they are demanded as proof of identity not only abroad but within the United States as well, displacing driver’s licenses as the primary form of identification in everyday life.
- They become the template for standardized versions of the driver’s license, turning them into a de facto National ID card.

Features such as the inclusion of a remotely readable RFID chip would greatly enhance the private sector’s tendency to piggyback on the perceived “trust value” of these documents. Although theoretically optional, like driver’s licenses and credit cards before them, they may quickly become what are for all practical purposes requirements for navigating through the modern world. The result would be a situation where the government gains a tremendous new power to track and control the movement of citizens.

Or innocent citizens, at any rate. We must always keep in mind that as the perceived “trust value” of such documents rises, and as their adoption becomes more widespread, the payoff for counterfeiting them also rises—perhaps even more steeply—with the result that counterfeit or fraudulently acquired real documents will continue to remain available to determined and well-financed wrongdoers.⁵

While we understand the desire of the ICAO to increase confidence in travel documents, reduce fraud, combat terrorism, and protect aviation security, the inclusion of RFID tags will have disproportionate and unnecessary effects on privacy and civil liberties. Developed without outside input, the ICAO passport has morphed from a simple identity document to become a de facto monitoring device. Worse, this monitoring device threatens to be foisted on the American public with little or no debate. Because of the power and potential of RFID chips, the actions of the ICAO threaten the rights of Americans and people around the world.

CONSUMER ISSUES

The second major area where privacy concerns are raised by RFID tags in addition to government uses is the commercial side. Major retailers are engaged in a major push to advance adoption of RFID technology, and many envision RFIDs eventually replacing UPC bar codes on products.

Such a pervasive adoption of RFID technology raises profound privacy questions. The most detailed and often intimate picture of Americans’ lives can be constructed through their consumer purchases. The issues were well explained in a position statement issued by a coalition of 30 consumer and privacy organizations.⁶ They include:

- **Hidden placement of tags.** RFID tags can be embedded into/onto objects and documents without the knowledge of the individual who obtains those items. As radio waves travel easily and silently through fabric, plastic, and other materials, it is possible to read RFID tags sewn into clothing or affixed to objects contained in purses, shopping bags, suitcases, and more.
- **Unique identifiers for all objects worldwide.** The Electronic Product Code potentially enables every object on earth to have its own unique ID. The use of unique ID numbers could lead to the creation of a global item registration sys-

³See e.g. Kevin G. Hall, “Brazil ratifies fingerprinting, photographing of U.S. visitors,” Knight Ridder, Feb. 12, 2004; available online at <http://www.miami.com/mld/miamiherald/news/world/americas/7934565.htm>.

⁴Rachel L. Swarns, “Millions More Travelers to U.S. to Face Fingerprints and Photos,” New York Times, April 3, 2004.

⁵See James Moyer, “Security Document Theory White Paper,” online at <http://www.cfp2004.org/spapers/moyer-sdt.pdf>.

⁶“RFID Position Statement of Consumer Privacy and Civil Liberties Organizations,” November 2003, available online at <http://www.aclu.org/SafeandFree/SafeandFree.cfm?ID=15559&c=207>.

tem in which every physical object is identified and linked to its purchaser or owner at the point of sale or transfer.

- **Massive data aggregation.** RFID deployment requires the creation of massive databases containing unique tag data. These records could be linked with personal identifying data, especially as computer memory and processing capacities expand.
- **Hidden readers.** Tags can be read from a distance, not restricted to line of sight, by readers that can be incorporated invisibly into nearly any environment where human beings or items congregate. RFID readers have already been experimentally embedded into floor tiles, woven into carpeting and floor mats, hidden in doorways, and seamlessly incorporated into retail shelving and counters, making it virtually impossible for a consumer to know when or if he or she was being “scanned.”
- **Individual tracking and profiling.** If personal identity were linked with unique RFID tag numbers, individuals could be profiled and tracked without their knowledge or consent. For example, a tag embedded in a shoe could serve as a de facto identifier for the person wearing it. Even if item-level information remains generic, identifying items people wear or carry could associate them with, for example, particular events like political rallies.

Given the potential for widespread commercial use of RFID chips, we believe that Congress ought to step in and require privacy protections surrounding the use of this technology—in particular, the incorporation into law of the fair information principles that are recognized around the world.

GOVERNMENT PRIVACY AND CONSUMER PRIVACY: NOT SO SEPARATE

Although I have distinguished the privacy issues raised by the government’s adoption of RFID tags and the private sector’s, the difference between the two is quickly eroding from the perspective of individual privacy. Government security agencies are increasingly making an effort to make use of private sector information in anti-terrorism efforts that are oriented around vast sweeps through Americans’ data in the hunt for terrorists. And the government’s power to access private data is rapidly expanding through the Patriot Act and other measures.

In general, privacy concerns are more serious when they involve the government. But increasingly, the information that is collected about people by a retailer or other private-sector corporation can and is ending up in the hands of the government.

CONCLUSION

I believe that all the testimony you hear today will make clear that RFID chip technology is growing rapidly and has incredible potential for both use and abuse. I hope that my testimony has amplified two further points: this growth is taking place largely outside of the control of the US government and it will have significant impact on every American. What that impact will be has yet to be decided.

Congress must be vigilant and involved in how RFID technology is deployed. What is at stake is no less than how and when Americans will be identified and tracked here and around the world. We are at a pivotal juncture, where technology has presented us with the ability to implant monitoring devices on everything. And their use is being contemplated on perhaps the most fundamental travel document in the world. All without any guidance or direction from Congress or the American people.

The decisions Congress makes on RFID chips will affect the direction of this technology around the world. You must decide whether we want to go down the path of incorporating RFID into our identity documents or to choose a less invasive technology like the two-dimensional bar code. Over the longer term, the Congress needs to consider how the fair information principles that my fellow panelists have discussed can be applied to RFID and the many other new technologies that have placed us on the edge of becoming a surveillance society.

The debate must begin right now. If RFID technology is to be employed it must be carefully controlled, yet none of those controls currently exist. A fait accompli, presented by an unelected international body, is a real possibility. We urge you to be vigilant in monitoring these developments and creating legal controls to protect American privacy both domestically and internationally. Thank you.

Mr. STEARNS. I thank the gentleman.
Mr. McLaughlin.

STATEMENT OF MARK McLAUGHLIN

Mr. McLAUGHLIN. Thank you, Mr. Chairman. Good afternoon, Mr. Chairman, and members of the subcommittee. My name is Mark McLaughlin. I serve as the Senior Vice President for VeriSign's Naming and Directory Services Division. I'm very appreciative to have the opportunity to be here this afternoon. By way of background, VeriSign is the leading provider of critical infrastructure services for the internet and telecommunications networks.

Every day, VeriSign processes 10 billion domain name lookups and e-mails, provides internet security for thousands of corporations, processes 25 percent of all North American electronic commerce and facilitates billions of daily phone calls and millions of daily SMS messages.

I am here today to talk about VeriSign's role in the EPC network which is our selection as the root operator for the Electronic Product Code network. As mentioned, an Electronic Product Code embedded on an RFID tag provides a unique number that could be assigned to cases and pallets within the supply chain for identification. With the EPC network, computers that use RFID technology to identify objects can acquire associated information about that object, enabling manufacturers to track items and materials throughout the supply chain.

VeriSign was selected to operate this network by EPCglobal, a nonprofit joint venture of the Uniform Code Council which manages the allocation of bar codes and EAN International, which provides similar services internationally. They are responsible for driving the global adoption and implementation of the EPCglobal Network across various industry segments.

VeriSign's role in making the network work is building and operating the Object Name Service, ONS. Building and operating the EPC network is a very comfortable fit for VeriSign. We have over a decade of experience operating a proven, secure, global platform for the .com and .net domain name naming system. VeriSign also brings a strong record of securing internet commerce and communications. These will be critical to the success of the EPC network.

The EPC system works very much like the internet's Domain Name System. VeriSign, as I mentioned, operates the system worldwide for .com and .net. Like the Domain Name System which appoints web browsers to a server where they can download the websites for any particular web address, ONS will point computers looking up EPC numbers to detailed product information stored on the distributed network. The system leverages the power of today's internet, through a distributed architecture that will enable individual companies to share information about products in more than one secure data base on the web.

VeriSign's experience will help the EPC network deliver integrated services that allow each company in the supply chain to authenticate themselves on to the network, allowing producers, wholesalers and retailers to share secured product data in real-time.

Through the use of the EPC network, businesses can become more efficient and productive in logistics, inventory management and product placement. To support this new model for supply chain

management, thousands of enterprises need to be able to securely access, in real-time, potentially billions of unique EPCs from a highly available global ONS directory. As other people have mentioned, the cost savings and efficiencies throughout this system are vast. VeriSign's involvement with EPC network will help ensure that the system is run with real-time accuracy and security.

Around the issue of consumer privacy, an important thing to do note is about the tag itself, as other people have mentioned. Much has been said and written about concerns that somehow reading a tag on a product will give away sensitive information about a consumer. That's not the case. The tag simply does not supply any information about a consumer. As a matter of fact, the tag doesn't contain any information about the product itself. That information is stored on data bases. Having said that, VeriSign is committed to working with all groups, especially privacy groups, to ensure secure and reliable network. That is our legacy on the internet that we are excited to bring to the EPCglobal network as well. More specifically, we will provide our leading digital certificate technology to help ensure that only authorized parties will be allowed access to information on the network. These are exactly the same kind of certificates that we use to protect billions of online transactions every day. Additionally, our encryption technologies are employed to encrypt transmission of any information that is deemed to be sensitive. This technology will also be used to help prevent snooping and hijacking and other forms of intrusive behavior.

VeriSign takes our role in RFID technology as seriously as have taken our role in supporting the internet's continued growth. I appreciate the opportunity to testify before the subcommittee this morning and I'd be happy to answer questions later.

[The prepared statement of Mark McLaughlin follows:]

PREPARED STATEMENT OF MARK MCLAUGHLIN, SENIOR VICE PRESIDENT, NAMING AND DIRECTORY SERVICES, VERISIGN, INC.

Good morning Mr. Chairman and Members of the sub-committee. My name is Mark McLaughlin and I serve as Senior Vice President for VeriSign's Naming and Directory Service division. VeriSign is the leading provider of critical infrastructure services for the Internet and telecommunications networks.

Every day VeriSign supports 10 billion domain name lookups and emails, provides Internet security for thousands of corporations, processes 25 percent of all North American e-commerce and facilitates billions of daily phone calls and millions of daily SMS messages.

I am here today to talk about VeriSign's selection as the root operator for the Electronic Product Code network. An Electronic Product Code (EPC) embedded on an RFID tag provides a unique number that can be assigned to individual items in cases and pallets within the supply chain for identification and tracking. With the EPC network, computers that use RFID technology to identify objects can acquire associated information about that object, enabling manufacturers to track items and materials throughout the supply chain. This technology will revolutionize the way products are manufactured, sold and bought.

VeriSign was selected to operate this network by EPCglobal, a non-profit joint venture of the Uniform Code Council (which manages the allocation of bar codes) and the EAN International (which provides similar services internationally) responsible for driving the global adoption and implementation of the EPCglobal Network across industry sectors.

VeriSign's role in making the network work is building and operating the Object Name Service, or ONS. Building and operating the EPC network is a comfortable fit for VeriSign. VeriSign has over a decade of experience operating a proven, global platform for the .com and .net domain name system. VeriSign also brings a strong record of securing Internet commerce and communications that will be critical to the success of the EPCglobal Network.

The EPC system works much like the Internet's Domain Name System VeriSign operates as the authoritative directory for all .com and .net internet addresses.

Like the Domain Name Addressing system (DNS), which points Web browsers to the server where they can download the Web site for any particular Web address, ONS will point computers looking up EPC numbers to detailed product information stored on the network. The system leverage the power of today's Internet, through a distributed architecture that will enable individual companies to share information about products in more than one secure database on the Web.

VeriSign's experience will help the EPC Network deliver integrated services that allow each company in the supply chain to authenticate themselves onto the network; allowing producers, wholesalers and retailers to share secured product data in real-time.

Through the use of the EPC Network, businesses can become more efficient and productive in logistics, inventory management and product placement. To support this new model for supply chain management thousands of enterprises need to be able to securely access, in real-time, potentially billions of unique EPCs from a highly available global ONS directory. The possible cost savings and efficiencies throughout the system are vast with this technology. VeriSign's involvement with EPCglobal will help ensure the system is run with real-time accuracy on a secure platform.

Around the issue of consumer privacy, the most important thing I can tell you is about the tag itself. Much has been said and written about concerns that somehow reading a tag on a product will give away sensitive information about a consumer. That is not the case. The tag does not supply any information about a consumer. Having said that, VeriSign is committed to working with all groups, especially the privacy groups, to ensure a secure and reliable network. That is our legacy on the Internet that we are excited to bring to the EPCglobal network.

More specifically, we will provide our leading digital certificate technology to ensure that only authorized parties will be allowed access to information on the network. These types of certificates are also used to protect billions of online transactions. Additionally, encryption technologies can be employed to encrypt transmission of any information that is deemed to be sensitive. This will prevent snooping and hijacking.

VeriSign takes our role in RFID technology as seriously as we have taken our role in supporting the Internet's continued growth. Thank you for the opportunity to testify before the sub-committee this morning.

I am happy to answer any questions you may have today or in the future as we move forward with this important technological innovation.

Mr. STEARNS. I thank the gentleman.

Mr. Laurant.

STATEMENT OF CÉDRIC LAURANT

Mr. LAURANT. Good afternoon, Mr. Chairman, and members of the subcommittee. My name is Cédric Laurant. I'm Policy Counsel with The Electronic Privacy Information Center or EPIC which is based in Washington and is a public interest research and advocacy organization that focuses on emerging civil liberties issues.

I appreciate the opportunity to testify before the subcommittee today on RFID technology. I will talk about the impact that the RFID technology has on people's privacy, new risks that are created by this technology, what opinion polls show on consumers' perception of RFID, legislative developments in the United States and the world, the need for legal framework based on fair information practices and finally, our recommendation to the subcommittee.

The debate over RFID technology touches upon many controversial policy issues. At its most fundamental, widespread use of RFID tags could enable corporations to track every move consumers make. Corporations which compile data which is submitted by the tags could determine which product a consumer purchases, how often products are used and even where the product, by extension of the consumer travels. By aggregating data to form con-

sumer profiles, corporations could make inferential assumptions about a consumer's income, health, lifestyle, traveling habits, buying habits, etcetera. This information could then be sold to governments to create a dossier of individual citizens or simply sold to other corporations for marketing purposes.

With the ability of RFID readers to collect data from tags, once a consumer has left the store moves beyond the reader's range is currently limited. RFID technology is quickly advancing, while measures to protect individual privacy by limiting the amount and type of information corporations can collect about consumers is lacking.

There have been several cases in the past year where the technology of RFID has been used without informing consumers. In the retail industry, for example, some retailers have collected information from customers without providing them with the most basic notice. But an even more significant problem then, the notification of the presence of tags to customers in stores, what may happen is the possibility of consumers being covertly tracked, profiled and in other ways monitoring the tags they purchased outside the store premises.

It's also important to note that RFID systems of all kinds are capable of generating a volume of consumer data several orders of magnitude greater than has been possible before. Numerous retail industry white papers refer to the coming bonanza of high resolution information and the ease with which this information could be shared with third parties and aggregated for further data-mining. The indiscriminate use of personal identifiable information is already a significant issue to consumers as numerous surveys have shown. As the RFID application moves into widespread use, this problem will only become serious.

Public opinion polls consistently find strong support among Americans for privacy rights and law to protect their personal information from government and commercial entities. Opinion polls have also demonstrated that there is clear support for the meaningful protection that clear privacy principles like the fair information practices provide. Several recent polls show that Americans are highly concerned about their privacy and that legislation is preferred over self-regulated programs.

In the case of RFID, despite growing media coverage, consumers are generally not aware of RFID. A recent study conducted by Cap Demme Group and the National Retail Federation found that 77 percent of the more than 1,000 consumers surveyed were not familiar with RFID. Of those that were familiar, less than half had a favorable perception of the technology.

The on-going support for the right of privacy is not surprising. Privacy protection has a long history in the United States. The United States has a strong tradition of extending privacy rights to new forms of technology. Congress has repeatedly sought to protect people against new privacy risks that new technologies brought.

It was never the intent to prohibit the technology when Congress legislated or to prevent the growth of affected business models. Instead, the purpose was to establish public trust and confidence in the use of new technologies that had the ability to gather a great

amount of personal information and if used improperly to undermine the right of privacy.

I will skip the part about recent legislative development in the U.S. and the world, but I suggest you take a look at the full version that is in the record.

Legislation is needed because consumers have shown in polls that they view self-regulation is insufficient to effectively protect their privacy and the RFID industry needs simple, predictable and uniform rules to regulate the collection and use of information through the user of RFID technology. This legal framework could be based on the fair information practices.

I won't detail what those fair information practices are since a witness, Paula Bruening, has already talked about them.

The public debate about whether to regulate RFID technology raises the same questions that previous new technologies collecting personal information had raised in the past. Congress, by regulating RFID technology and by adapting the fair information practices to this new technology would follow the tradition of providing people with basic rights to protect their privacy and the use of their personal information.

We recommend basically that Congress should first rule on legislation specifically targeting the use of RFID in the retail sector and require clear labeling and easy removal at item level, rather than tagging on individual consumer product. Then Congress should legislate in a way that protects consumers from improper use and sharing of data in both the public and private sector by establishing a legal framework based on clear information practices.

Thank you very much for your attention.

[The prepared statement of Cédric Laurant follows:]

PREPARED STATEMENT OF CÉDRIC LAURANT, POLICY COUNSEL, ELECTRONIC PRIVACY INFORMATION CENTER

My name is Cédric Laurant. I am Policy Counsel with the Electronic Privacy Information Center (EPIC) in Washington. EPIC is a public interest research and advocacy organization that focuses on emerging civil liberties issues.¹ I also am the editor of the 2003, and upcoming 2004, *Privacy and Human Rights* report², an annual survey of privacy laws and privacy-related developments in over 65 countries in the world.

I appreciate the opportunity to testify before the Subcommittee today on RFID technology.

1. Impact of RFID technology on people's privacy

Radio Frequency Identification (RFID) is a type of automatic identification system that enables data to be wirelessly transmitted by portable tags to readers that process the data according to the needs of a particular application. Tags in use today are small enough to be invisibly embedded in products and product packaging. The data transmitted by the tag may provide identification or location information, or specifics about the product tagged, such as price, color, or date of purchase. RFID readers are often connected to computer networks, facilitating the transfer of data from the physical object to databases and software applications thousands of miles away and allowing objects to be continually located and tracked through space. RFID may also be used to identify documents and currency. RFID may even be deployed to identify individuals. Today, major uses of RFID include supply chain management, animal tracking, and electronic roadway toll collection.

¹ More information about EPIC is available at the EPIC web site <http://www.epic.org>.

² <http://www.privacyinternational.org/survey/phr2003/>.

1.1. *New risks for privacy*

The debate over RFID technology touches upon many controversial policy issues. At its most fundamental, widespread use of RFID tags could enable corporations to track every move consumers make. Corporations which compile the data transmitted by the tags could determine which products a consumer purchases, how often products are used, and even where the product—and by extension the consumer—travels. By aggregating data to form consumer profiles, corporations could make inferential assumptions about a consumer's income, health, lifestyle, buying habits, and travels. This information could be sold to governments to create dossiers of individual citizens, or simply sold to other corporations for marketing purposes. While the ability of RFID readers to collect data from tags once a consumer has left a store or moved beyond the readers' range is currently limited, many consumer groups and privacy advocates note that RFID technology is quickly advancing, while measures to protect individual privacy by limiting the amount and type of information corporations can collect about consumers is lacking.

There have been several cases in the past year where the technology of RFID has been used without informing consumers. In the retail industry, for example, some retailers have collected information on their customers unbeknownst to them without providing them with the most basic notice.

Between March and July of 2003, shelves in a Wal-Mart store in Broken Arrow, OK, were equipped with hidden electronics to track lipstick products. Consumers at the store were unaware of the RFID tags contained in the lipstick and that they were being viewed 750 miles away by Procter & Gamble researchers in Cincinnati who could tell when the lipsticks were removed from the shelves and could even watch consumers in action thanks to a system of video surveillance installed in the store. Researchers had concealed the RFID readers in contact paper placed under the shelves and had embedded RFID antenna chips in the lipstick packaging.³

Gillette, the razor manufacturer, has tested smart-shelf technology in conjunction with major retailers such as Tesco in which a hidden camera took pictures of shoppers whenever they picked up razor blades from the shelf, and again when they pay for the item at the check-out counter. The smart shelves were tested at a Tesco store in Cambridge, England.⁴ Planned testing in Brockton, MA, was publicly canceled by Wal-Mart after consumer protest.⁵

But an even more significant problem than what may happen in stores is the possibility of consumers being covertly tracked, profiled and otherwise monitored via live RFID tags in products they own. There are already a number of RFID applications in use worldwide which offer tracking and monitoring of individuals as part of their explicit feature set. Many of these applications make use of passive RFID tags similar to what might be used in consumer products. A significant portion of data generated over a product's lifetime will be stored in a centrally-managed, Internet-accessible database known as the Object Name Service (ONS). If information in this database is associated with personally identifiable information, the potential for abuses of consumer data and individual privacy will dwarf any technology previously in use.

Moreover, it is important to note that RFID systems of all kinds are capable of generating a volume of consumer data several orders of magnitude greater than has been possible before. With in-store deployment, it is predicted that Wal-Mart will generate more than seven terabytes of RFID data a day.⁶ Numerous retail industry white papers refer to the coming bonanza of high-resolution consumer information and the ease with which this information could be shared with third parties and aggregated for further data mining.⁷ The indiscriminate use of personally identifiable information is already a significant issue for consumers in the US, as numerous surveys have shown. As RFID applications move into widespread use, this problem will only become more serious.

³"Chipping away at your Privacy," Chicago Sun Times, November 9, 2003, available at <http://www.suntimes.com/output/lifestyles/cst-nws-spy09.html>.

⁴Alok Jha, "Tesco Tests Spy Chip Technology," Guardian, July 9, 2003, <http://www.guardian.co.uk/uk—news/story/0%2c3604%2c1001211%2c00.html>.

⁵Alorie Gilbert and Richard Shim, "Wal-Mart Cancels 'Smart Shelf Trial,'" ZDNet.com, July 9, 2003, <http://zdnet.com.com/2100-1103—2-1023934.html>.

⁶Mark Palmer, "Overcoming the challenges of RFID," ZDNET.com, February 27, 2004 <<http://zdnet.com.com/2100-1107—2-5165705.html>>.

⁷See, for example, "Sponsored Feature: A Vision for RFID In-Store Consumer Observational Research," RFIDNews.com, October 20, 2003, available at <http://www.rfidnews.org/weblog/2003/10/20/sponsored-feature-a-vision-for-rfid-instore-consumer-observational-research/>.

1.2. Consumer surveys

Public opinion polls consistently find strong support among Americans for privacy rights in law to protect their personal information from government and commercial entities.⁸

Opinion polls have also demonstrated that there is clear support for the meaningful protections that clear privacy principles, like the Fair Information Practices (FIPs) provide. A number of recent polls show that Americans are “highly concerned” about their privacy and that legislation is preferred over self-regulatory “trust” programs.

When polled Americans indicate that:

- Individuals should be in control of both initial collection of data and data sharing. The public considers opt-in—the principle that a company should obtain an individual’s affirmative consent before collecting or sharing data—as one of the most important privacy rights.
- Individuals want accountability and security. Individuals report that they want the ability to obtain redress for privacy violations and think that it is important that access to data within an entity be limited.
- Individuals want comprehensive legislation, not self-regulation. Americans report that the current self-regulatory framework is insufficient to protect privacy and favor new federal legislation to protect privacy online.
- Individuals value anonymity.
- Individuals do not trust companies to administer personal data and fear both private-sector and government abuses of privacy.
- Users want notice of how their personal information is collected, used, and with whom it is shared.

In the case of RFID, despite the growing media coverage, consumers are generally not aware of RFID.

A recent study conducted by Capgemini Group and the National Retail Federation found that 77% of the more than 1,000 consumers surveyed were not familiar with RFID.⁹ Of those that were familiar with RFID, less than half (42%) had a favorable perception of the technology, while 31% had no opinion.

An internal Proctor & Gamble survey, not intended for public dissemination, found strong negative reaction to RFID use.¹⁰ A document describing the November 2001 survey was located on an unsecured Auto-ID center server and publicized by CASPIAN. 317 consumers participated in Internet-based survey sponsored by Auto-ID center and Proctor & Gamble. 78 percent of respondents reacted negatively. The major findings were as follows:

- More than half claimed to be extremely or very concerned;
- “Big Brother” is used in 15 separate cases to describe the technology;
- Consumers did not want “smart tags” in their homes;
- The reassurance that the “tags” could be turned off and privacy guaranteed was not compelling.

This ongoing support for the right of privacy is not surprising as privacy protection has a long history in the United States. The US has a strong tradition of extending privacy rights to new forms of technology. Congress has repeatedly sought to protect people against the new privacy risks that new technologies brought. Congress enacted privacy laws for the telephone network, computer databases, cable television, videotape rentals, automated health records, electronic mail, and polygraphs. In each case, it was never the intent to prohibit the technology or to prevent the growth of effective business models. Instead, the purpose was to establish public trust and confidence in the use of new technologies that had the ability to gather a great amount of personal information and, if used improperly, to undermine the right of privacy.

The new technology of RFID raises important privacy risks for people. Those risks point to the urgent need to establish protections for personal information collected by RFID to safeguard consumers’ privacy interests.

2. Recent legislative developments

2.1. In the United States

There is currently no federal law applicable to the collection and further processing of personally identifiable data gathered through RFID technology. Legislative

⁸See EPIC’s Public Opinion on Privacy web page reviewing those opinion polls on a regular basis at <http://www.epic.org/privacy/survey>.

⁹Beth Bachelder, “Study: RFID Not Well-Known By Consumers,” *InformationWeek*, June 24, 2004, available at <http://www.informationweek.com/story/showArticle.jhtml?articleID=22101950>.

¹⁰Auto-ID Center/Proctor & Gamble Survey, available at <http://cryptome.org/rfid/pk-fh.pdf>.

developments in various States indicate that state legislatures are aware of their constituents' concerns for the privacy risks that RFID technology raises.

Some state legislation has been proposed, but not yet passed, in several state legislatures over the past year. Most of this legislation includes provisions for clear labeling of consumer products bearing RFID tags, a requirement originally proposed for federal legislation drafted by consumer advocacy group CASPIAN (Consumers Against Supermarket Privacy Invasion and Numbering), the "RFID Right to Know Act of 2003."¹¹ RFID bills drafted in the US, (except for a Virginia bill which merely calls for a general review of RFID practices and privacy¹²) all share a "notice" clause first articulated in RFID expert Simpson Garfinkel's RFID Bill of Rights and CASPIAN's RFID Right to Know Act of 2003.¹³ This clause requires any consumer products bearing RFID tags to be conspicuously labeled. A bill introduced, and still being debated, in the California senate requires that tags be destroyed or removed at checkout.¹⁴ A bill in the Utah legislature, which failed, and bills in Missouri and Maryland require tags be labeled only.¹⁵ There is no legislation currently being considered at the federal level, although the FTC recently conducted a workshop to debate the current and potential impact of RFID on consumers and individual privacy. Privacy advocates cautioned that without a framework of protection for personal information RFID use could have significant, negative impact on individual privacy.¹⁶

2.2. International landscape

Other nations already have regulations or guidelines that can help protect consumers against major privacy risks raised by RFID technology. Europeans have regulated privacy with an omnibus law that comprehensively protects the use and processing of personal information. Rules protecting personal information processed through the use of RFID technology are therefore already in place with two data protection directives (enacted in 1995 and 2002) that apply to both the issue of individual tracking and the association of data with personal identification. As a result, any use of RFID tags that involves the processing of personal data is likely to be subject to a number of data protection obligations.¹⁷ Further, the more recent Directive on Privacy and Electronic Communications states that "location data may only be processed when it is made anonymous or with the consent of the individual."¹⁸

Over the past year there has been widespread activity on the part of governments and NGOs to begin the process of regulating the use of RFID to protect individual privacy. Data protection and privacy commissioners in Sydney, Australia, adopted an international resolution on RFID. Several individual countries, including Italy, Canada, Australia and Japan, have outlined guidelines for domestic industry to follow in their use of RFID.

The approach of regulatory movements worldwide varies considerably. Although it does not explicitly call for labeling (instead, it calls for openness and transparency), the joint resolution of international data protection and privacy commissioners in Sydney, Australia in November 2003 is similar to the California bill in that it requires tags on consumer items to be able to delete data and destroy or dis-

¹¹ CASPIAN, "RFID Right to Know Act of 2003", available at <http://www.nocards.org/rfid/rfidbill.shtml>.

¹² Virginia House Bill 1304, available at <http://leg1.state.va.us/cgi-bin/legp504.exe?041+ful+HB1304>.

¹³ See Simson Garfinkel, "An RFID Bill of Rights," Technology Review, October, 2002, at page 35, available at http://www.simson.net/clips/2002.TR.10.RFID_Bill_Of_Rights.pdf and the "RFID Right to Know Act of 2003," available at <http://www.nocards.org/rfid/rfidbill.shtml>.

¹⁴ California Senate Bill 1834, available at http://info.sen.ca.gov/pub/bill/sen/sb_1801-1850/sb_1834_bill_20040401_amended_sen.pdf.

¹⁵ Utah House Bill HB 251, available at <http://www.le.state.ut.us/2004/htmldoc/hbillhtm/hb0251.htm>; Missouri Senate Bill 867, available at <http://www.senate.state.mo.us/04INFO/bills/SB867.htm>; Maryland House Bill 32, available at <http://mlis.state.md.us/2004rs/-billfile/HB0032.htm#Exbill>.

¹⁶ Radio Frequency Identification: Applications and Implications for Consumers, Federal Trade Commission Workshop, June 21, 2004, available at <http://www.ftc.gov/bcp/workshops/rfid/>.

¹⁷ Eduardo Ustaran, "Data Protection and RFID Systems," Privacy & Data Protection Volume 3, Issue 6, at page 6, available at http://www.berwinleighton.com/download/PDP-RFIDtag_simplifications.pdf. Article 8 of the EU Data Protection Directive of 1995, for example, prohibits the processing "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life." EU Data Protection Directive 95/46/EC, Official Journal of the European Communities of 23 November 1995 No L 281 p. 31, available at http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31995L0046&model=guichett.

¹⁸ EU Directive on Privacy and Electronic Communications 2002/58/EC, Official Journal, OJ L 201, 31.07.2002, p. 37, available at http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf.

able tags.¹⁹ Joint guidelines released by Japan's Ministry of Public Management, Home Affairs, Posts and Telecommunications (MPHPT) and the Ministry of Economy, Trade and Industry (METI) on June 8, 2004, call for consumers to be given options on how they might interfere with the reading of tags but appear to say nothing about rights to have the tag removed or destroyed.²⁰

3. Need for a legal framework based on Fair Information Practices

Legislation is required because consumers have shown in polls that they view self-regulation as insufficient to effectively protect their privacy, and the RFID industry needs simple, predictable and uniform rules to regulate the collection and use of information through the use of RFID technology. This approach is consistent with US privacy legislation.

This legal framework could be based on the Fair Information Practices. The Fair Information Practices are a set of rights and responsibilities developed in the early seventies. They help ensure personal information is not used in ways that are inconsistent with the purpose for which they were collected. Fair Information Practices typically include the right to limit the collection and use of personal data, the right to inspect and correct information, a means of enforcement, and some redress for individuals whose information is subject to misuse. Fair Information Practices are in operation in laws that regulate many sectors of the US economy, from companies that grant credit to those that provide cable television services. Your video rental store is subject to Fair Information Practices as are public libraries in most states in the country. The government itself is subject to the most sweeping set of Fair Information Practices: the Privacy Act of 1974, that gives citizens basic rights in the collection and use of information held by federal agencies and imposes on these same agencies certain obligations not to misuse or improperly disclose personal data.

The current debate about whether to regulate RFID technology raises the same questions that previous new technologies collecting personal information had raised in the past. Congress by regulating RFID technology and by adapting the Fair Information Practices to this new technology would follow the tradition of providing people with basic rights to protect their privacy and the use of their personal information.

The Fair Information Practices would provide clarity and promote trust for consumers and businesses. They would also encourage the RFID industry and retailers using RFID technology to develop better techniques to protect privacy. If all stakeholders can rely on a set of clear and stable rules to guide their use of RFID, it is likely, in the long term, to reduce the need for government intervention.

3.1. Recommendations

Legislation should protect consumers from improper use and sharing of data in both the public and the private sector. The legislation would address all forms of RFID-based services, from travel security to employee monitoring, child tracking and amusement park patron management. Congress should rule on legislation specifically targeting the use of RFID in the retail sector and require clear labeling and easy removal of item-level RFID tagging on individual consumer products. Clear labeling and easy removal of tags will ensure that consumers receive proper notice of RFID systems and are able to confidently exercise their choice whether or not to go home with live RFID tags in the products they own. Notice and choice are in fact two key components of the Fair Information Practices and elements that consumers value, as shown in many opinion polls. Consumers without high levels of technical capability have no way of knowing if a "killed" tag is merely disabled, physically destroyed, or in fact still fully functional. Tag removal, on the other hand, is transparent and 100 percent effective.

In our comments to the Federal Trade Commission (attached as an appendix to this testimony), we limit our recommendations to the private sector and to the use of RFID technology in the retail industry. We recommend a comprehensive assessment of RFID technology and global practice and recommend the FTC to publish and disseminate documents that educate the general public about RFID technology and with the purpose of educating businesses about RFID technology and the importance of protecting individuals' privacy.

¹⁹ See International Conference of Data Protection & Privacy Commissioners "Resolution on Radio-frequency Identification," Final Version, 20 November 2003, available at <http://www.privacyconference2003.org/resolutions/res5.DOC>.

²⁰ "Japanese RFID Privacy Guideline Released," June 8, 2004, RFIDBuzz.com, available at http://www.rfidbuzz.com/news/2004/japanese_rfid_privacy_guideline_released.html; see also Nikkei BP news article, June 8, 2004, available at <http://nikkeibp.jp/wcs/leaf/CID/onair/jp/flash/312386> (in Japanese).

3.2. EPIC's RFID Guidelines

EPIC has drafted a set of industry guidelines which adapt the Fair Information Practices to RFID technology. The guidelines allow businesses in the manufacturing and retail sectors to adopt the technology in a wide range of applications while protecting consumer's basic privacy interests. The guidelines require users of RFID systems to refrain from linking personally identifiable information to RFID tag data whenever possible and only with the individual's written consent. The guidelines also prohibit the tracking or profiling of individuals via RFID in the retail environment; require tags and tag readers to be clearly labeled; and stipulate that tag reading events be perceptible to the consumers through their association with a light or audible tone. We suggest that these guidelines serve as a basis for new federal legislation governing the use of RFID in the retail sector.

Failure to establish strong safeguards in law has generally resulted in economic harm to commerce and growing public concern on privacy. The key to protecting people from the new challenges the RFID technology raises for their privacy is to ensure the effective enforcement of Fair Enforcement Practices or similar privacy principles. We suggest you to consult the RFID guidelines provided in the appendix to this statement when considering privacy legislation for RFID.

Thanks you for your attention to the privacy implications of RFID. We look forward to working with the Committee on this and other issues.

Mr. STEARNS. I thank the gentleman.

Mr. Molloy.

STATEMENT OF JOHN MOLLOY

Mr. MOLLOY. Good afternoon, Mr. Chairman and subcommittee. Thank you very much indeed.

I am John Molloy. I'm the Managing Director of a company called ViaTrace. We provide global traceability solutions to government and industry throughout the world.

What I would like to share this morning is real life of RFID can do, what I believe RFID can do and why it is good.

At the moment, within agriculture in the U.S., there's an issue, the identification and tracking of animals. And first let me say, U.S. is leading the way by its early adoption of RFID in this area. Eight years ago in Parliament in EU, the EU addressed a similar issue as to how do we do this, how do we trace it? Luckily, I was in the Parliament that day and we started a consortium and we researched the issue for 55 man years. The largest research project ever. How do we do this? How do we move control? Even then RFID was suggested as being the way forward.

Subsequent to that, we've actually commercialized and made a product, ViaHerd which is available which will address some of the issues that USDA have.

RFID and why it's good. We have an issue and I'm going to quote some numbers. They're not exact numbers, but we have a real business issue. The business issue is we have 96 million head of cattle, okay? And we need to know who they are. Very simple thing. So we have the following, simple traceability. We're going to identify the animal. His name is John, he's born today. That animal is going to be fed for 3 months. He's going to be sold to another farmer who is going to feed him for 3 months and he's going to be sold to another farmer and so it goes on and eventually he ends up in slaughter. It's very simple. Okay?

But we've got 96 million. And that 96 million is going to move over 2 years, so we've actually got 288 million transactions per year. Okay? We've got to do it because there's a problem. So we're going to do what we do in Europe and in a lot of cases this is what

we do in Europe. We employ a lot of people. We go out into the field. We say hello, cow, here's a tag, here's a number, it's unique. We fill in a piece of paper, we bring it back in and we bring that piece of paper to a bureau and they type it, like that. Ninety-six million.

And then another 30 million, and then another 30 million because you have to record the movement, otherwise you can't trace. We can't report. And that's actually what happens.

I'm going to give you another idea. You go out and electronically—put a chip in his ear, we're doing it. Put a chip in his ear. The animal moves, a reader reads it, the record is sent. The animal moves, the reader reads it, the animal is sent. Why do we do it? God forbid, there is disease within the animal kingdom. We know this. This is an issue. We want to protect health. We want to protect business, but there is disease.

In a paper-based system and this is proven, 2 weeks ago in the U.K., the U.K. Commons Committee slammed their own internal system. Bad data. Inaccurate data. They lost 1.2 million animals in 2 years. That's a lot of animals to lose in 2 years.

Three weeks ago in France we all of a sudden discovered 30,000 BSE cases in the last 10 years. Never recorded, because it's paper. Everything points to its paper.

Mr. STEARNS. BSE is Mad Cow?

Mr. MOLLOY. Yes, BSE is Mad Cow Disease. In the scenario that I want to build you, you can only build traceability based on when you need it, okay? It's 9 o'clock in the morning in Nebraska and a veterinarian has just discovered that an animal has foot and mouth disease. It's another disease. We don't want to eat it. It's bad, okay? At 10 o'clock in the morning in Chicago an animal walks into the abattoir. This guy has already been notified and this guy is all together. This animal will be turned away in an RFID situation because the data is flowing. If I'm waiting for paper, I'm waiting 3 weeks.

Three weeks, 4 weeks, this is fact. Fifty two million pounds foot and mouth cost to the U.K. Because they had paper. I urge you, America, this is the opportunity to lead the world in traceability and animal identification. RFID is good. We would not run a business on inaccurate data. We wouldn't run a healthcare system on inaccurate data. Data collection, RFID is the greatest enabling technology for the collection of data, for the betterment of business and the betterment of people.

Thank you.

[The prepared statement of John Molloy follows:]

PREPARED STATEMENT OF JOHN MOLLOY, MANAGING DIRECTOR, VIA TRACE

Good Morning. I am John Molloy, Managing Director of ViaTrace—a provider of traceability solutions to government and industry worldwide.

As a father and businessman who is personally involved with, and affected by, the privacy and technology issues being addressed by the Committee today, I applaud the Committee's leadership in examining them.

I would also like to thank the Committee for the opportunity to offer my thoughts this morning, and will begin by briefly sharing my first-hand experiences in developing and implementing a multi-national, RFID-enabled traceability system across Europe's Agriculture sector.

In response to several widespread disease outbreaks that put the lives and wellbeing of tens of thousands of families and farmers at risk—not to mention a cru-

cial, multi-billion dollar agriculture sector—the European Union embarked on the most extensive research and development initiative ever undertaken into livestock movement and disease control. This European Commission funded project leveraged the resources of six nations, and took the equivalent of 55 person-years to complete.

Our company, ViaTrace, was selected to utilize the research from this project to design and implement a pan-European animal traceability system known today as ViaHerd.

The singular purpose of ViaHerd is to protect the public health and the agriculture sector that every citizen depends on.

Designed as a multi-national, “farm-to-fork” traceability system, ViaHerd’s success ultimately rests on the successful collection and cataloging of terabytes of information.

The information that ViaHerd collects is available to a variety of users based on their credentials, roles, and responsibilities. For example, a farmer can quickly access and analyze information about his herd, but he cannot access information about his neighbors herd.

Whereas, veterinary officials would have access to a much more limited data set and only for specific reasons, like during the time of an emergency, or crisis situation (when the need to quickly and accurately reconstitute a herd can mean the difference between life and death).

An emergency situation would be declared based on two scenarios: an airborne disease outbreak, (like FMD) or the identification of a genetic disease (like BSE).

In order to effectively locate all of the animals a single cow came in contact with requires that a host of information is recorded in a standardized format each time the animal is moved, or medicated.

For example, in the US there are roughly 96 million cattle, of which about one third are brought to slaughter each year.

An effective system would capture information about where the animal was born, where it was raised, which medications it received, when and by which veterinarian. Considering the providers of this information—generally farmers and veterinary officers—are often “in the field,” the business challenge for us was to make the collection of this information as timely, accurate, and efficient as possible.

ViaTrace often relies on RFID technology to achieve this objective.

Once the data is accurately captured, it must be formatted into a standardized structure, like the product classification a bar code provides. The structure has to be both rigid and dynamic. Rigid in the sense that, like the debit and credit structure of the banking world, there must be full accountability and compliance. For example, if an animal were sold from one producer to another, the system must show that it was both sold and purchased. Dynamic in the sense that it must show who transported it and by what route (this can vary based on any number of conditions).

Therefore, considering the billions of animals bought and sold each year for human consumption, coupled with the increased risk of bio-terror, airborne and genetic diseases, efficient, comprehensive data capture tools—like RFID tags—are practically a global trade requirement.

The EU plans to implement a pan-European electronic animal identifier system by 2006.

At that point, the system will not only gather information from electronic readers of individual animal tags, but will also include an electronic identifier management module. Say for example the electronic identifier is in the form of an ear tag. In addition to registering the tags themselves, ear tag suppliers and distributors could be registered, along with the individuals authorized to apply ear tags to animals (farmers, veterinarians, control assistants, etc).

The system would then monitor the distribution and use of ear tags prior to their application to animals, assisting in the audit, control and the re-ordering process to help prevent fraud and loss of revenues to government agencies.

This layering of information is important because the sheer volume of transactions in a 40 nation trade zone invites the possibility for both inaccurate data and increased fraud—both issues are in direct conflict with ViaHerd’s intended objective of protecting the public health and welfare.

ViaHerd’s sophisticated data capture and authentication technologies balance business needs with privacy concerns and legislative requirements.

Today, any nation, producer, or veterinarian that uses our system, is automatically fully compliant with all EU agriculture, trade, and privacy laws. This is good for business—but it is even more important for the protection of public health.

Therefore, it is our belief that RFID is a critical component of any system that relies on timely and accurate data.

I would like to offer a few lessons we have learned through the development and implementation of ViaHerd, which I believe may be relevant to your inquiry:

- Protecting the public's health while safeguarding global trade—is a delicate balance that *can* be and has been realized
- Cooperative action involving government and industry is the ideal model for action, since it is critical to protect the public health in a way that strengthens rather than burdens the agriculture sector
- Preparatory action—taken *before* the specter of mad cow disease infects our supermarkets, school lunchrooms, and homes—is possible and vital.

A fully evolved RFID-enabled animal registration system is one of the keys to providing stable and sustained international commerce. The United States has an opportunity to embrace this technology to the benefit of all stakeholders.

In light of its intentional design to meet public health, business, legislative and privacy priorities, I hope the ViaTrace technology will serve as a useful model for your consideration.

In closing, I thank the Committee again for its leadership and hope the Committee finds the experiences of ViaTrace to be of value. All of us at ViaTrace stand ready to be a resource as you work through this challenging issue.

I appreciate your time and attention, and would be happy to answer any questions you may have at this time.

Mr. STEARNS. I'll start the questions here.

Mr. Laurant, you know, I think the hearing is to find out, we all agree that the future is enormous for this technology, but the question would be is the pervasiveness of the privacy of the individual and how to be protected.

Mr. Laurant, on your webpage, privacy webpage, it says "RFID systems enable tagged objects to speak to electronic readers over the course of a product's lifetime from production to disposal, providing retailers with an unblinking, voyeuristic view of consumers' attitude and behavior, purchase behavior."

My question is to Dr. Sarma, is that true, do you think that's true what they have on their website? Is that possibly—

Mr. SARMA. The range of RFID tags is extremely limited as you saw today.

Mr. STEARNS. And in fact, without the intent of the piece of sand, the grain of sand, it's not going to work, is that true?

Mr. SARMA. So without the antenna, the tag doesn't work. The range is very limited.

Mr. STEARNS. And the antenna, you take off?

Mr. SARMA. If you want to reactivate the tag when you purchase it, in any case you couldn't read it and more fundamentally, we are—this is an evolving technology. And companies that are using RFID in the U.S. today are just on the threshold of starting to make it work. It's got to be engineered. You've got to engineer your truck and then you can get it to work.

Pervasiveness assumes a certain technology performance that we're really years and years away from.

Mr. STEARNS. That statement is probably not accurate today, from a technological standpoint.

Mr. SARMA. I would consider it an exaggeration.

Mr. STEARNS. Do you want to answer? We're saying the MIT scientist says exaggeration.

Mr. LAURANT. It's an exaggeration if you apply it to current technology, but as Mr. Sarma said, the technology is evolving every day. So it wouldn't be—

Mr. STEARNS. Then Dr. Sarma, how far are we away from this statement being possibly accurate?

Mr. SARMA. The range of RFID tags is always going to be limited because very fundamentally, tags we're talking about EPC tags and

I can only speak for EPC, in the supply chain are passive tags. In other words, they have no battery.

Mr. STEARNS. Right.

Mr. SARMA. And they're limited to physics on how much power you can—there are also legal limits from the FCC on how much power a reader can put out. In a passive tag, it can only respond physically from a certain distance. So unless you carpeted a city, a State with readers, your visibility into these things is going to be very limited. And even if you carpeted a city or a State with readers, your ability to read through water, through metal, as you saw in the demonstration through fabric also makes it such an unreliable way of tracking. There are other means you would prefer if you wanted to do that.

Mr. STEARNS. Can it—like in bad weather, like you have snow or ice, does it read through that?

Mr. SARMA. It is very difficult to do it reliably.

Mr. STEARNS. Okay. Now someone has mentioned to me that China is at the threshold starting an EPC global network, that China would set the standard. So any of you would like to comment on the idea that we in the United States probably should work to set the standard immediately or we'll be left with China setting the standard for the world and what does that mean?

Mr. SARMA. I have not seen anything official from China, but I've heard about speculation that China may do something and it is very important, I think, on two fronts. First of all, it's very important that there be a single global standard because if Procter & Gamble makes a product and it wants to sell it in Egypt or in the United Kingdom, it will be good and very efficient for Procter & Gamble if the standards are the same, first of all.

The second thing is that RFID is a technology that fundamentally endows an enterprise with efficiency. And it's very important for the United States and its economy to be efficient and to take the lead in efficiency. So from both points of view, it will be better if (a) the U.S. took a lead; and (b) if all countries around the world use the same standard.

Mr. STEARNS. Mr. Steinhardt, can you give me what current government uses of RFID technology raise privacy concerns in your opinion? Are they actually being implemented and just, in general, if there's not any on the present horizon, what do you fear in the government uses?

Mr. STEINHARDT. The current, as I said in the testimony, the current uses are—by the government are fairly limited. They are, for example, the use in libraries or proposed use in libraries of book—

Mr. STEARNS. Let's say we go ahead and have it in the libraries. Then everybody would have a record of everything—or if we had it at Blockbusters or a video store that everybody had, that would be in the private sector. But in the government, if you go to the Library of Congress and they have it, then everybody has an idea of what you're—

Mr. STEINHARDT. It means, for example, that if we don't take the proper precautions, that anyone can determine what it is that you are carrying out of the library and can track you, for example, at a political rally. It could track what you have in your pocketbook

or have in your backpack. But the thing that I tried to focus on this morning was really, I think, the question, the issue that the Congress would look at very carefully is the proposed use of RFID chips in identity documents and specifically at the proposed use in the passport. The ICAO process, International Civil Aviation Organization, is a process that the United States government set forward. This is not hypothetical. It's not—it's a little obscure, but it's not exotic. This is a process we set forward. Our government is actively engaged in it. That issue is going to come back to the Congress at some point. It will have to come back to the Congress at some point, but it may come back as a *fait accompli*. You may be hearing well that's the global standard. The global standard is now we have passports and passports contain RFID chips. It's too late for the United States government to do anything about it. What we're urging is that the Congress get out ahead of the curve and look carefully at the use of RFID in identity documents.

Mr. STEARNS. Okay, my time has expired.

The gentlelady.

Ms. MCCARTHY. Thank you, Mr. Chairman. I'm honored to fill in for Ms. Schakowsky and follow up on some of the issues that we both share. I want to thank everyone for being here today. This has been very illuminating for all of us.

I'd like to follow up with Ms. Hughes and Ms. Bruening on where we go from here.

In your testimony, Ms. Hughes, you talk about the pilot testing on pallets and shipping, but you don't mention the testing with lipstick. And I am aware of the article from the Chicago Sun Times last year about the lipstick issue at the Wal-Mart. And it is of concern to me that we explore that just a little bit more.

Ms. Bruening, you call for consumer privacy concerns being addressed in a baseline privacy legislation which I agree. The government has been wise to stand back and let all of you experts grapple with this, but I think we need, Mr. Chairman, further conversation about what a baseline privacy bill might do to address some of the good things that are going on, as well as some of the things that are not in the best interest of consumers or the privacy laws that we all cherish.

So let me start with you, Ms. Bruening. Would you expand a little bit on what you'd like to see in a baseline privacy legislation.

And then back to Ms. Hughes on how do we do the testing that industry needs that will help the consumer without infringing on privacy issues that I know you respect as well?

Ms. BRUENING. Thank you. In calling for baseline privacy legislation, CDT is acknowledging that we have been involved in this conversation, all of us, repeatedly over the last few years. Every time there's a new emerging technology that involves data collection, we find ourselves back in these hearing rooms talking about how to specifically address privacy and that specific technology.

Our belief is that if we have legislation that addresses collection of information no matter what the technology, we will be way ahead of the curve when it comes to the next technology that emerges. Businesses will have a better sense of what the responsibilities are in terms of putting privacy—implementing policies that are privacy respectful and consumers will have a better sense

of what they can expect in terms of their rights and responsibilities and their own information.

What we're calling for is baseline legislation that incorporates elements of fair information practices. These well-established principles that have formed the basis of our U.S. Privacy Act of 1974, that have been the basis of industry guidelines, international agreements on data flows and data protection, these are well established, well trusted now and we think that they should form the basis of any privacy legislation going forward.

And I think what we would do is reduce the need to keep having to come back and have this discussion repeatedly every time there's a new technology that comes out.

Ms. MCCARTHY. Thank you very much, Ms. Bruening.

Ms. Hughes?

Ms. HUGHES. Yes, thank you, Congresswoman, I appreciate the opportunity to really set the record straight on this lipstick test. You were referring to a test that P&G and Wal-Mart conducted in a store in Oklahoma in the spring of 2003. The purpose of this test was to really test the technology for supply chain management on the shelf. If you think about lipstick packages, they're in a little tray by color and to be able to find them in the right place when the consumer wants them is really important. So we were testing the accuracy of the technology.

The tag was actually on the lid of the carton that the lipstick goes into, so it would be thrown away as the lipstick was removed. There was full notice at the shelf about electronic surveillance and that tags would be used on the shelf in the Wal-Mart store.

We also had webcams that were looking at the shelf so that we, in Cincinnati, could actually see the accuracy of the technology. It was focused at the shelf, at the trays of lipstick and frankly, when a consumer got their head or their hand in the way it really interrupted our test. So there was no other readers in the store. It was just for that particular test. There was no way to know if a consumer was there, who they were or anything else about it. So for us, it was really an opportunity to test that technology.

And the point is that the camera was in full view and with that notice, we feel that there would be any opportunity if a consumer had a question, they could go to the customer service center, there's a customer service desk at Wal-Mart, but over that 4-month period, not a single consumer raised a question.

Ms. MCCARTHY. Let me ask since I didn't do opening remarks, I'm still not clear, what is the purpose of knowing what color of lipstick that particular consumer is buying? Is this a marketing tool now?

Ms. HUGHES. It's really a supply to demand. So it's like what are the—to make sure that the products are in the right place when the consumer wants them and at the right price. So if you're looking for a particular color that you were used to having, but you couldn't find it because it wasn't in the slot where it's supposed to be, you might go elsewhere or you would purchase another lipstick that was from another manufacturer.

So in this case it was to test the technology to see if we could actually see whether those lipsticks were where they were supposed to be on the shelf the way that the consumer wanted them.

You know, if you've bought lipstick sometimes people will look at them and they'll put them in different places, so it's not where that color is supposed to be. It gets a little frustrating.

Ms. MCCARTHY. I understand now better the intent. In the good old days we had real human beings that checked the shelves from time to time and made sure they would answer questions that consumers had on the spot and make sure the products were available.

I hope you realize that what we're trying to look at is the fine line between good intentions and not so good intentions that really do trample upon those things that we view as important such as privacy.

Ms. HUGHES. And I think if I may just agree with Ms. Bruening that for us what's really important is to give that notice to consumers when there is an EPC tag in place and part of the EPC global usage guidelines that we've put in place do have that as one of the mainstays following the information practices. In addition, that there would be choice for consumers where they can discard it and in this case with the lipsticks it was very easy because it was on the carton.

Ms. MCCARTHY. Well, I think what we're about here is to make sure that in the good old days when you sought out someone with a question so you could get an answer and better choose your product, that was willful. A camera which they may or may not take the time to read the print that says it's watching you is not the same effect on an individual. That fine line is what we're trying to grapple with in the legislative process of how to do the best for the people that we all want to serve.

I thank you for your explanation. Thank you.

Mr. STEARNS. I thank the gentlelady.

Mr. Issa.

Mr. ISSA. Thank you, Mr. Chairman. I probably have a little different perspective than some of the members and my questions may be a little toward that history of my company has used barcodes for decades. We've used RFID. And I'll just run through something and then pose it as a single question.

Since RFID has been used by the CIA, the FBI, all of our intelligence organizations for decades, obviously, not a small piece, but generally a transceiver or some other product, we've tracked fish and other wildlife using RFID. My own company and UPS and others have used various both RF and non-RF schemes for pallet and individual shipping information. Containers at sea right now are being mandated by the Federal Government to be tracked so that we can determine that they have not been opened and where they are at all times.

Since RFID is in all the new Toyotas and Lexuses that are out there and since package information as anti-theft product from many companies has been around for a long time and as we all know, having walked in and out of places, isn't always disabled when you leave because the next time you go in somewhere you go whoops!

And since our very own spyware legislation that's being worked on this committee speaks to a similar situation of identity and private information being gathered and trying to prohibit it, are we legitimately dealing with your problem relative to all the other col-

lection data, all the other storage information and now my question, if so, isn't this really more a matter of us legislating what you do with the information, how long you can keep it and what is appropriate, rather than the question of whether or not you can initially collect it?

I'd like to hear from pro and con because that's obviously my view is that this is part of a bigger picture. There is nothing unique about what you're doing and there's nothing new about what you're doing. We're simply talking about it being easier and greater in more numbers and thus data bases—we have to ask how long can data bases be kept linked to individuals?

Ms. Hughes, I'd like to include you in this.

Ms. HUGHES. Well, for us, we have as part of our privacy policy that we keep data only as long as it's needed. So to create the transaction, to fulfill it or whatever. This is for consumer information that we would collect to better understand consumers' needs and desires for products and services. For example, if they have signed up to be a matter of one of our newsletter subscriptions or some other type of service that we provide on one of our brands, then we would keep it as long as they decide that they want to be part of that. So it's a pure opt-in and when they want out, then we take them out and we do not keep that longer.

Mr. ISSA. And you would consider that if we codified that in the law, that would be fine?

Ms. HUGHES. Yes, although as far as legislation, I think as far as RFID it's premature for that, but if that would be the case, yes.

Ms. DILLMAN. Just the only thing I would add is I'd absolutely support what you had to say. Our greatest concern, we absolutely support protection of private information, personal information, but we don't believe that data collected by RFID should be different. We believe there needs to be a single standard for all personal information, no matter how it's collected. And if we created an environment where every new technology or every medium has a different requirement, it will be a nightmare to actually support and maintain.

Mr. ISSA. Anyone else want to weigh in, particularly on the question of whether this is unique and different and requires specific legislation or more broadly should be addressed as harvested information, personal identity?

Mr. STEINHARDT. If I can, Congressman, I think there are two questions there. First is whether or not this is unique. I think that as Paula Bruening said earlier, every time a new technology come down the pike we have this conversation. I don't think that RFID—it has some unique properties to it, but I do think it's part of the larger mosaic of technologies that enable the surveillance of individuals, a collection of data about individuals, not simply about cows or shipping pallets; and that over-arching legislation is necessary here. We can no longer take the approach that we've taken in the United States which is the sectoral approach where a particular issue comes before the Congress and you do or don't legislate, so we have, for example, very good legislation that deals with our video rental records which was the result of the disclosure of Judge Bork's records during his confirmation hearing. We don't

have particularly good legislation in this area and many other areas.

I do think we need over-arching legislation. I agree with industry that they need one set of standards that may apply differently in different circumstances and may reach different results in different circumstances, but I do agree with the one set of standards, but they need to be in laws. It's too late for us to simply say that we're going to wait until every technology comes down the pike is mature because every day we face a new technology and we need to set the standards now.

Mr. ISSA. Mr. Chairman, I know my time has expired.

Mr. STEARNS. Does anyone else wish to answer his question?

Ms. BRUENING. I'd just like to comment that I think that from the perspective of the development of technology, you end up with a better result if you have that kind of baseline privacy legislation that focuses on the information itself. I've been peripherally involved in the discussions about spyware and I think it's a really clear demonstration of how difficult it is to do the kind of line drawing you need to do in writing legislation whereas if we had that kind of baseline law we could avoid a lot of this sort of tortured conversations that go on to try and figure out what falls in and what falls outside of the line of what's covered by the law.

I think that in the instance of RFID, we would be very concerned about implementing legislation specific to RFID too early because it would impact the development of the legislation and skew the way it progressed. But if we had that kind of privacy law in place, we could feel a lot more confident as the new technology goes forward, that it was being developed in a privacy respectful fashion. Thank you.

Mr. STEARNS. Anyone else like to answer the question?

Mr. LAURANT. Yes, I would like to point to the European rules on privacy. The European regulator did not need to redraw a new law to address the specific privacy issues raised by RFID. They have a directive that they enacted in 1995 that can take care of the problem and can answer most privacy issues that consumers may have regarding RFID.

Mr. STEARNS. The gentleman's time has expired.

Mr. ISSA. Thank you, Mr. Chairman.

Mr. STEARNS. Mr. Strickland.

Mr. STRICKLAND. Thank you, Mr. Chairman. I want to thank the committee. This has been very interesting and a thoughtful discussion. I think the reference to the spyware legislation is appropriate because I have been concerned that as we consider spyware legislation we focus on legislation that limits technology rather than limits bad or inappropriate behavior. And it seems to me that we're facing perhaps the same kind of choice when it comes to this discussion this morning.

I'm also sitting here wanting to give a commercial to a bill that my colleague, Dr. Norwood, and I have introduced in an attempt to stop the diversion of drugs, prescription drugs. We've introduced what we are calling the Prescription Drug Abuse Elimination Act which would mandate the use of RFID track or trace or some other technology for Schedule I and Schedule II controlled substances by the year 2008. And it seems to me that this could be a very helpful

and appropriate application of this technology, because of the horrendous problem we have in this country of Oxycontin and other controlled substances being diverted from their intended prescribed appropriate usage.

So I would just like to ask you, Ms. Hughes, I know that Procter & Gamble is involved in this pilot project and I talked with Cardinal Health earlier this morning about their concerns, another great Ohio company, as well as Procter & Gamble and could you just say a little more about the pilot project and what you hope you can learn from it?

Ms. HUGHES. Yes, for us, as you, we feel like it's very important to be able to manage the inventories and prevent drug shortages, as well as the counterfeit drug program that's going on. So in this test along with a number of other drug manufacturers and retailers, we're supported by the FDA, as you know, for this test. And we feel like it's a powerful tool to deal with expiration date management, for example, diversion, reduction in medication errors, product security, etcetera. So we feel like there's a real opportunity for this and that's why we're testing the technology.

We appreciate your enthusiasm for introducing legislation.

Mr. STRICKLAND. and I would encourage my colleagues here. It's a very bipartisan bill. Dr. Norwood, as you know, has a medical background. He's a dentist by training and this is a huge problem and I think this could be a partial solution certainly.

If I can just ask Mr. Steinhardt a question. Your testimony was very interesting and taken to I guess what I would use the word extreme, alarming. You talked about eventually being able to track where every American citizen was and so on. I'll ask something that may be not terribly germane to this circumstance, but I've been concerned that we've had so many of our soldiers taken hostage and I've wondered why we can't develop some technology, maybe related to this technology or some use of this technology that would enable us at last to soldiers who are in combat areas or places of extreme danger for abduction to somehow be tracked so that we can know where they are if they are taken hostage and would you just comment on that or anyone else that knows this technology well enough to indicate to me or to us if such an approach would be feasible or possible.

Mr. STEINHARDT. Let me reassure you, Congressman, that I don't think anybody on this panel, including the representative of the ACLU, none of us is suggesting that this is technology that should be smashed in its infancy. There are legitimate uses of RFID. One legitimate use may be to use it with our military so that they can, in fact, be tracked.

I saw a news article just this morning that raised some interesting questions that the Attorney General of Mexico has chosen to have an RFID chip implanted under this skin, along with members of his staff, apparently, because there are kidnappings of high government officials in Mexico. That may be an appropriate use of the technology and there are other technologies that might make sense.

The question that I raise by my testimony is whether we want to put it in an identity document that is carried by millions of Americans or potentially if it were going to driver's licenses by the vast majority of adult Americans.

Mr. STRICKLAND. And I appreciate your answer and then if I can just ask the good doctor, as the academic expert here, do you think such a technology could, in fact, be helpful in the situation such as I described with our soldiers?

Mr. SARMA. I think that's a very good question, Congressman Strickland. I think the challenge, however, is that the particular tags we're talking about, the EPC tags that I described, unfortunately have a very limited range.

Mr. STRICKLAND. Sure.

Mr. SARMA. Only about ten feet as we demonstrated. So it wouldn't be applicable in that scenario. However, other technology like Lowjack, car theft device, active technology which have tags which have batteries and can actually transmit, could be adapted. But I think that's a different technology than the one we're talking about here.

Mr. STRICKLAND. I was assuming that was probably the case. And if I can just ask one more quick question—

Mr. STEARNS. The gentleman is entitled to 3. You waived your opening statement, so you are entitled to 2 more minutes.

Mr. STRICKLAND. I appreciate you being so gracious. There have been references made here to a global or an international standard on how EPC could or should be utilized and I'm just wondering if any of you would like to offer a suggestion as to where you think those standards should be developed and how they would be developed and enforced?

Mr. SARMA. I'd be happy to address that, Congressman. I think that like the internet which is a way of transmitting data, RFID is a way of lubricating the supply chain and keeping track of material in the supply chain. Today, an item might spend months, 30 weeks in the supply chain, and if you're going to keep track of things in the supply chain, for example, if Procter & Gamble manufactures something in the U.S. and it's being sold offshore in some country, and Procter & Gamble wants to make sure that there is no counterfeiting, there is no theft, wants to make sure that it keeps its inventories low, but at the same time it can meet the demand in this foreign country, it would be ideal if all the standards were exactly the same so that, in fact, global commerce could operate in a very similar way to the internet or the worldwide web. And this is something that EPC Global has spent a great deal of time internationally through its member organizations around the world promoting and we're very close to clinching the deal, if you will, of a single global standard.

Now the U.S. has always been an innovator in the barcode community and in RFID and it has played a very important role in this and much of the initial sponsorship came from the U.S. but some of it came from around the world, but it is a global standard we're shooting for.

Mr. STRICKLAND. You've been very gracious, Mr. Chairman, I yield back.

Mr. STEARNS. All right, the gentleman from Arizona, Mr. Shadegg.

Mr. SHADEGG. Thank you, Mr. Chairman, and I would like to echo the comments of Mr. Strickland. This has been a fascinating discussion. Actually, the entire concept of having this type of tech-

nology in the consumer product line and throughout our economy is fascinating and to some of us who aren't as technologically as advanced as we might be comes as king of a whole new shock.

I want to talk a little bit about some things that I think are similar and some things that I think are different between that and which the technology that's out there right now. For years now, many of us have gone to the grocery store and been offered the choice of taking advantage of this little discount if we're willing to surrender a degree of privacy by saying yes, you can keep track of what groceries John Shadegg and his wife and his family buy. That's a choice we make.

It seems to me this is a challenge because this does not involve my control of that circumstance. This now involves somebody else's control of that circumstance. And even though the technology, Dr. Sarma, suggests that this is only going to be readable for 10 feet or so and once I'm out the door it's not readable, one of my concerns is that if we do not educate the public of that fact, they're going to resent this or fear it, perhaps even irrationally fear it. And so it seems to me that although the technology has great advances, we need to carefully look at it so that we provide consumer assurance that their privacy is not invaded to too great a degree.

So I guess I'm inclined to go along with Mr. Issa's suggestion that perhaps a part of this is looking at control of the data.

One of my concerns about your comment, Ms. Hughes, so long as needed, I'm afraid that for those who have a distrust of commerce, then they conclude as needed as too vague a definition for each to make.

Let me ask both you, Ms. Hughes, and Dr. Sarma and also I guess, Mr. Molloy, given the tremendous value of this type of technology, what are the things that we should do to facilitate it coming to the market and not see the technology squashed by an over-reaction to the invasion of privacy issues?

Ms. HUGHES. Well, let me just start first, Congressman. I appreciate the question and just to clarify when I said before, the collection that I mentioned of data and how long we keep it is for our consumer marketing area when consumers have opted in to give us their information and how long we keep it is based on how long they want to stay in or if we're fulfilling a transaction for them.

Mr. SHADEGG. I only think that you have to have a clearer definition of what "as needed" is because if you were allowed to define "as needed" and I'm not precisely sure when that means I'm out, I may—that may leave people more skeptical who may say look, I'm not going to get in. I'm afraid you're not going to reasonably define "as needed."

Ms. HUGHES. We also have as backup for that, you know, a period of time where we say we would keep it for 2 years, for example. So if we haven't heard back from a consumer or we haven't had any interaction, then we would delete that. So we've got a period of time that's our backup then for retention.

But in this particular area for RFID and EPC, in particular, we wouldn't be collecting or having any information on consumers anyway as a manufacturer or for Procter & Gamble we have no need or no interest for that and—

Mr. SHADEGG. So you would not keep the information by consumer?

Ms. HUGHES. No.

Mr. SHADEGG. You'd keep gross data?

Ms. HUGHES. Right. All we are interested in is the aggregation of what products are being used, how often they're being used, the turnover for that so that we can better improve our supply chain and make sure that that product is where it needs to be. So as far as consumers for RFID and EPC, we haven't got any reason and no plans to have any consumer information.

Mr. SHADEGG. But I assume that you, or at least others on the panel would say if we were to disallow the retention of any personally identifiable information that would be overly restricting the data or is that not the case?

Ms. HUGHES. I'm sorry, could you rephrase?

Mr. SHADEGG. In other words, if we said yes, you may collect it, but only in the aggregate, not that John and Shirley Shadegg bought whatever it is, this Procter & Gamble product, but that this store sold these many units of that product—

Ms. HUGHES. Right.

Mr. SHADEGG. If that were the restriction, I believe that would be going too far in restricting the use of this type of technology. Or would you not agree with that?

Ms. HUGHES. Right, I mean as far as aggregation of data, you know, keeping data for some purpose that we're doing that, whether it's to do analysis or whatever, and we don't have any consumer information there, so as far as retention of that information it's for doing that analysis and we'll keep it for—

Ms. HUGHES. I think Safeway either keeps or uses it on my family for marketing purposes so they can sell me other products.

Dr. Sarma?

Mr. SARMA. Congressman, I think your comments are absolutely spot on. I think the key thing here is education because there are a lot of misunderstandings about what this technology is and it isn't. And the reason is it fits into a larger continuum of similar technologies that—

Mr. SHADEGG. As Mr. Issa pointed out.

Mr. SARMA. Right.

Mr. SHADEGG. When he started to say well, it's been around forever, I thought well, that's crazy and then you think about it for a moment he's absolutely right. It has been around for a very long time.

Mr. SARMA. And EPC is actually a very small and actually a very unsophisticated technology. Now for example, there are some who might say this can spy on me. What does a spy do listens to what I'm saying and then tells somebody else. EPC tag, all it does is I'm a bottle of shampoo. It goes to someone else. I'm a bottle of shampoo. It doesn't actually repeat anything.

Another misunderstanding is it knows where I am. The tag doesn't. The tag only knows it's a bottle of shampoo. It doesn't know where I am. It doesn't know where I've been. Now I think that education is very key. The second comment is the tag by itself actually doesn't gather any personal data. That's an independent thing.

Mr. SHADEGG. Right.

Mr. SARMA. I think that that clarification and these clarifications are very important because then people understand, consumers understand why this is very important.

Now finally, I'll say that when information is kept about individuals, it may be necessary for regulatory reasons, for example, to recall a medicine or to recall a packet of meat that's suspect and that's why I think that this sort of legislation, the discussions come up. It's premature to talk about it. It's really far away from figuring out how this technology is going to impact the world. It's a much simpler technology than people, I think, think it is.

Mr. SHADEGG. Mr. Molloy, did you want to comment Mr. MOLLOY. Yes, personally, technology is good and technology is bad and I actually do see the conflict. But I physically and personally believe that RFID is good because it allows you to react to situations. One of the examples, the example I gave of food, there was a report this morning that says America's beef industry is open to bioterrorism. That's a very vague report, but it may be true, but if we have something that can actually react to that, that actually saves lives. My feeling is that's good. Saving lives is good. Not eating meat that's going to kill you is good.

I understand then that how much data do you actually want to store. I'll give you a simple example. You want to store enough data to actually react. That's my argument. How long do you want to keep it for, that's entirely up to what's agreed. Thank you.

Mr. SHADEGG. I appreciate that. Mr. Chairman, I appreciate your indulgence. I want to conclude by simply saying on spyware one of the issues I was concerned about was the issue of stroke recording which truly is just like eavesdropping, it's like listening to your phone conversation because you can go into my computer and see every stroke I make on my computer. You are, in fact, eavesdropping on me and it's very much different than this technology which just says this is a bottle of shampoo that's going out the door at this moment.

Thank you, Mr. Chairman.

Mr. STEARNS. We're probably going to do another quick second round here. So my colleagues are welcome to stay. I'm just going to do a couple of questions and then we'll be able to go to you.

Ms. DILLMAN, the cost of implementing RFID, it's in the collection of the data, I guess. These exceptionally large amounts of data that's being collected, what happens to this data and is not the true cost impediment, not the tags, but the data tracking itself?

Ms. DILLMAN. That tends to be a common discussion, even in the industry and among our suppliers. And what I can tell you is how we have—what our implementation looks like and how we've addressed that issue.

If you actually recorded every single read and tried to store it somewhere locally, it would be a massive undertaking.

We don't need all of that data. We need an interpretation of the data to actually add value. So we don't need to know every point a case was read. We need to know where it ended up, that it's out on the sales floor or it's in the back room. And what we do is we filter the data and only pass through the conclusions that we really need.

We've encouraged every one we deal with to take a simplistic approach like that and that means it's a very doable implementation. It makes it very reachable for anyone.

Mr. STEARNS. Now Mr. McLaughlin, I just had a question. You talked about counterfeiting. Will RFID technology, we know it's useful in counterfeiting, but is it also that you can copy a tag and thereby counterfeit a package?

Mr. McLAUGHLIN. It would be possible to copy a tag, but actually the network itself then would have a misread. There would be one extra in the system that would show up as an aberration. It would actually be very helpful in drug diversion if an extra item showed up where it wasn't supposed to be. You'd see that.

Mr. STEARNS. Mr. Molloy, is there any harm to the RFID in terms of the signals or anything, I guess this is a question for Dr. Sarma, too? I mean should consumers be concerned about having all this—

Mr. MOLLOY. Radiation in the air?

Mr. STEARNS. Radiation?

Mr. MOLLOY. I don't believe so. We've been using it for many, many years. I'm definitely not an expert on the whole technology.

Mr. STEARNS. Dr. Sarma?

Mr. SARMA. Mr. Chairman, I'm not a metal expert, but I can make a comment on the physics. RFID operates in three bands designated by the government called industrial, scientific, medical bands. The power and the frequency is regulated by the FCC for use in industry and scientific endeavors and medical endeavors. A lot of medical equipment actually operates on this band.

Mr. STEARNS. Mr. Galione, can you encrypt these chips? In other words, a lot of people are concerned about the privacy and they talked about protection of privacy, but can't all these chips or these tags be encrypted?

Mr. GALIONE. As I mentioned in my testimony, the smart cards are very much, there's some very sophisticated levels of encryption that exists today in order to protect that information about people. So now you're talking about, if you're talking about some encryption at the item level or for logistics, yeah, it can be done, but the economics probably don't justify doing it.

Mr. STEARNS. Could you kill the encryption too? Could you send a signal to the tag and then kill the encryption too?

Mr. GALIONE. Theoretically, that's possible, sure.

Mr. STEARNS. Mr. Molloy, does the government need to subsidize as we move beyond cows and things—who is doing it in Europe? Who is paying for all of this?

Mr. MOLLOY. In Europe, Europe and U.S. are obviously very different states. In Europe, it's paid for by the state, it's funded by the E.U. Having said that—

Mr. STEARNS. So the E.U. pays for all this, the tags, the collection of data and everything?

Mr. MOLLOY. Yes, that's a European funded project. Having said that, in Europe, it's been very slow to adopt RFID. There's legislation on the way that says we must have RFID and there's pilots going on in the U.K. and various other countries across Europe but in that way America is way ahead because you said this is the way they do it.

Mr. STEARNS. All right.

Mr. MOLLOY. Paid for by the government.

Mr. STEARNS. Mr. Issa.

Mr. ISSA. Thank you, Mr. Chairman, and perhaps to answer your question on the passive devices that most of these products are going to use, they don't really put anything out. It's going to be just like any time you walk pass an electric motor or any number of other devices that put out radio frequency, so that's the good news.

On the other hand, at 134 megahertz, you've got a proliferation of power from things like the new Lexus and Toyotas where they're trying to have a transponder type environment. So that is a great question for our subcommittee on that because we have a lot of bandwidth utilization. There is a question of how much additional noise flow we are raising.

I think I would just like to make sure that I'm clear on the benefit side of this. We've been talking completely about the problem side of it with the exception of a few who show how they could use them.

I look at this as obviously the example of tainted beef, the fact that Safeway can contact me and say you have a pound of meat that came from this State code where right now what happens is if you happen to be watching your local cable break-in from CNN every 15 minutes on the hour or whatever, you're going to get an opportunity to hear that there's a bad batch of meat and it's number such and such and if you write it down and go look, you might find out that you're about to have e. coli or something.

So I view that as a great asset. And it's an asset that's only possible if we do collect and retain for a period of time very specific information that includes that Mrs. Shadegg bought that pound of beef and took it home or that can of tuna and that's a tradeoff that I think the committee is going to have to weigh.

As someone who is a consumer electronics manufacturer with Philips on the board of the consumer electronics industry with me over the years and so on, I would love nothing better as a manufacturer than to know that Circuit City 4 days ago sold to Mrs. Carstays an installed Viper car alarm and thus that now becomes the registered user of that product and I don't have to wait for a warrant card. There is a concern about what I do with it. On the other hand, I view that as a plus.

Last, but not least, we mentioned software. The whole idea that every single CD and DVD in the very foreseeable future could, in fact, have a unique embedded serial number and thus the registration would be automatic and there would only be at any given time on the net one copy or whatever the Congress decides is fair use, another issue that this committee is dealing with.

So I for one am delighted to hear that across the panel there are concerns, but there's also a recognition that these and thousands of other uses make this a technology that we'd like to see happen. We'd like to see that two cent item inside a pair of socks, if we can get passed the other concerns.

And Mr. Chairman, it wasn't a question there, but I thank you for giving me a second round.

Mr. STEARNS. I thank my colleague for staying over and it's nice to have someone who actually has real world experience on the subcommittee and participating.

We're ready to close. Is there anything that all of you would like, anyone would like to add, anything that members have said? If not, we appreciate the patience in all the witnesses and I think we've had a very good hearing.

We are adjourned.

[Whereupon, at 1:27 p.m., the hearing was adjourned.]

[Additional material submitted for the record follows:]

PREPARED STATEMENT OF THE GROCERY MANUFACTURERS OF AMERICA

The Grocery Manufacturers of America (GMA) appreciates the opportunity to provide the food, beverage and consumer product manufacturers' perspective on the use of Radio Frequency Identification (RFID) technology. GMA and its member companies believe this technology offers benefits for consumers and acknowledge and share concerns regarding consumers' privacy as it relates to the use of this emerging technology. We are committed to working with the technology providers, consumers, the Administration and the Congress as RFID technology is implemented and more widely adopted.

GMA is the world's largest association of food, beverage, and consumer product companies. With U.S. sales of more than \$500 billion, GMA members employ more than 2.5 million workers in all 50 states. The organization applies legal, scientific, and political expertise from its member companies to vital food, nutrition, and public policy issues affecting the industry. Led by a Board of 42 Chief Executive Officers, GMA speaks for food, beverage and consumer product manufacturers at the state, federal and international levels on legislative and regulatory issues.

The Technology

For more than four years, the Auto-ID Center at Massachusetts Institute of Technology (MIT) has been developing supply chain applications for RFID technology that promise to deliver significant benefits to the economy and consumers. RFID has been around since WWII and is already used in many applications from the Speed Pass at the gas station to EZ pass at toll booths. RFID is the name given to the technology that involves tags that emit radio signals and devices called readers that pick up the signal. The electronic product code or EPC establishes a standards-based approach to using RFID technology to uniquely identify an entity or object that has an EPC tag attached to it. The EPC is essentially a radio enabled bar code, which can be read wirelessly. Other pieces of the EPC network enable the information from the tag to be analyzed and shared between supply chain partners.

The Auto-ID Center's work on the development of the EPC stands out as one example of how public, private, and academic interests can unite to support research and development, and help move technology forward to benefit society. The Auto-ID Center (now known as the Auto-ID Labs) is supported by many of the world's leading companies and organizations including many in the food, beverage and consumer products industry. EPCglobal, a joint venture between EAN International and the Uniform Code Council, was chartered last September to develop open, global standards for use of the EPC Network and currently has a subscriber base of more than 200 companies representing a cross section of major industries around the world. EPCglobal is responsible for the orderly adoption and implementation of the EPC system worldwide.

Similar to the license plate on a car, an Electronic Product Code (EPC) is a way to uniquely identify a pallet, case or individual product. It is the next generation of today's Universal Product Code (UPC), known commonly as the "bar code." Instead of the familiar printed strip, a tiny silicon chip holds a unique number that identifies a product. The tag, like today's barcode, cannot be read and understood without passing by a reader that is connected to a data infrastructure. The major improvement of EPC over the barcode is that it does not need "line of sight" to be read, but instead uses radio waves which makes the reading of transactions much faster.

Connected to a network, EPC technology will allow companies for the first time to manage their global supply chain in real time, at any time—offering never before available benefits. Some of those benefits include:

- Streamlining inventory control on a global scale;
- Deterring theft and counterfeiting;

- Keeping shelves stocked with products desired by consumers;
- Speeding the placement of new products; and
- Easing removal of expired products.

Though much of the research is focused on business and supply chain applications of the technology, the EPC ultimately promises consumer benefits as well. Consumers may see improved checkout procedures and customer service. Other benefits could include:

- Better availability of products; and
- Swifter and more effective food and product safety recalls.

It is also important to note that EPC technology can offer solutions to government, such as:

- Improved customs handling and border controls;
- Enhanced Department of Defense (DoD) logistics management; and
- Better security for moving luggage through airport terminals.

Within the food, beverage, and consumer products industry, RFID is a part of a broad range of e-commerce activities designed to make the supply chain more effective and efficient. From a manufacturer's perspective, some of the benefits of EPC/RFID include the elimination of manual counting and recounting of products in distribution. Warehouses, trucks, backrooms, and shelves will contain readers that will automatically and continually track products and maintain perpetual and accurate inventory data. Out-of-stocks—a problem which plagues the consumer packaged goods industry—could be virtually eliminated through preset triggers which would automatically call for replenishment. This would also allow for theft to be measured and controlled in real time, and will increase the ability to identify counterfeit products. Additionally, product recalls will be conducted in a much more efficient and effective manner through continuous monitoring of products throughout the supply chain.

Status of EPC/RFID Implementation

Currently, manufacturers are conducting pilot studies on the use of EPC/RFID in select warehouses, backrooms, trucks and manufacturing plants. While it is clear that broad implementation of EPC/RFID on individual items tracked to the store level is still years away, many retailers are eager to adopt case and pallet level tagging to enhance supply chain efficiencies. In addition, several manufacturers have been leading initiatives to use EPC/RFID to reduce theft in the supply chain, especially for high value goods, and look forward to realizing benefits from the day-to-day use of the technology.

As with any new technology, many hurdles stand between current capabilities and ultimate implementation. These include:

- Difficulty in reading radio frequencies through metals and liquids.
- Upgrading chip quality and consistency to improve read rates.
- Avoiding interference with other radio frequency technologies, such as those used in warehouses, manufacturing plants, stores, etc.
- Developing software to help sort vast amounts of data into meaningful information.
- Improving the ability to read all cases on a pallet.
- Making RFID affordable for many consumer product manufacturers.

These issues must first be addressed in a reliable and cost-efficient manner before we are likely to see widespread adoption of EPC/RFID.

Public Policy Issues

While EPC/RFID can produce major benefits, the technology also raises public policy issues that must be addressed in a proactive and responsible way. Chief among those issues are concerns about consumer privacy, which some legislators and advocacy groups are already trying to address by proposing legislation that specifically regulates RFID. GMA believes RFID-specific legislation is unnecessary because the existing legal framework, industry self-regulation, and market forces provide consumers ample protection against potential abuses of the technology. In addition, premature legislation could also inadvertently stifle many of the beneficial uses of this technology (food security, bioterrorism) as well as technological solutions to public policy concerns.

Under Section 5 of the Federal Trade Commission Act, the FTC has authority to regulate unfair or deceptive practices in and affecting commerce. In recent years, the Commission has used this authority to develop a substantial body of law regulating the manner in which businesses collect and use consumers' personal information, particularly online. In addition, the Commission enforces specific privacy laws such as the Children's Online Privacy Protection Act, the Fair Credit Reporting Act,

and the Gramm-Leach-Bliley Act. This body of law is readily applicable to consumer privacy concerns about potentially unfair or deceptive uses of RFID technology.

The protections of Section 5 of the FTC Act and other statutes enforced by the Commission are not technology-specific. Section 5 was not amended with the advent of radio or television, nor during the emergence of concerns about online consumer privacy. While there have been some laws enacted to deal with certain aspects of emerging technologies, FTC consumer protection enforcement, including enforcement of general consumer privacy protections, stems primarily from existing prohibitions against deception and unfairness. Specifically, the FTC has brought several consumer privacy cases on the theory that a company's failure to abide by its stated privacy policies constitutes a deceptive practice under the Act.

In conjunction with its enforcement activities, the FTC has long encouraged companies to make privacy policies available to consumers. Many of the retailers and manufacturers, who are at the forefront of implementing EPC/RFID, already publish and abide by privacy policies that provide consumers protection against misuse of their personal information. Retailers and manufacturers know that consumers, as well as the FTC, hold them to the promises made in their privacy policies. They recognize that it will be necessary to update these policies to notify consumers when EPC/RFID technology is in use, how they collect and use information from EPC tags, and any choices consumers have. Given that consumer trust is paramount in the branded consumer products business, it is very much in the manufacturers' interest to ensure that consumers are comfortable with this new technology and fully understand the privacy policies by which they abide.

State law enforcers and the plaintiffs' bar have also been active in the consumer privacy arena. Their cases, while arising from consumer protection principles similar to those found in Section 5, have often focused on violations of unstated policies, for example, the failure to disclose that consumer personal information has been shared with another company.

These precedents demonstrate that basic consumer protection principles such as deception and failure to disclose were able to evolve to protect privacy in the online context. With the framework already in place, these principles are readily applicable in the context of RFID. There is no reason to believe, even in the absence of a law that specifically mentions "radio frequency identification," that the Commission, state law enforcers, and the plaintiffs' bar will stand by in the face of abuses of RFID technology. Like the internet, RFID is simply another method by which consumers and businesses can share information. Any privacy concerns it raises are virtually identical to those raised by information collection on the internet, and the same solution should apply; *market forces and government encourage businesses to provide privacy policies, and the promises contained in those policies are enforced.*

Self-regulation has an important role in encouraging responsible use of EPC/RFID. In January 2004, the GMA Board of Directors formally adopted privacy guidelines established by EPCglobal. They are available at www.epcglobalinc.org. The guidelines will continue to evolve as technological applications and consumer opinions develop, but they already address important aspects of a sound privacy policy—consumer notice, choice, and education, as well as records use, retention and security. Specifically, the guidelines focus on the need for consumer notification and choice when RFID tags are present in or on products available for purchase. In addition, they affirm companies' commitment to use, maintain, and protect records generated though EPC/RFID in compliance with all applicable laws, including privacy laws.

Of course, even in the absence of legal and self-regulatory incentives, retailers and manufacturers have ample incentives to deal fairly with their customers. Retailers and manufacturers of brands rely on repeat business. Repeat business depends on consumer confidence in the seller. Thus, when a shopper goes into a supermarket for a favorite brand of food, the whole supply chain recognizes that the shopper's trust in the businesses that brought that brand to the market is critical to his or her decision to return again and again. In addition, manufacturers have invested hundreds of millions of dollars to create consumer confidence, trust and loyalty to their brands. It is, therefore, in the industry's interest to act responsibly when implementing this new technology in order to maintain that trust.

Some believe that we need new laws to address RFID. Enacting laws and promulgating regulations now would likely do more harm than good. New laws specifically regulating RFID could stifle development of the technology before its benefits are fully recognized. Since the currently-known benefits of the technology arise in interstate commerce, a patchwork of state regulations of RFID would be particularly problematic. The appropriate approach is to monitor the situation and assess whether there are privacy concerns that legitimately arise as this technology develops and then ask whether they are concerns that cannot be addressed through industry self-

regulation and the application of the unfairness and deception principles of the FTC Act.

Thank you for the opportunity to provide our perspective on this emerging technology. As the industry adopts EPC/RFID, we are committed to doing so in a way that protects consumer privacy and offers consumer benefits. We look forward to working with the Committee on this and other important issues in the future.

PREPARED STATEMENT OF THE RETAIL INDUSTRY LEADERS ASSOCIATION

The Retail Industry Leaders Association (RILA) appreciates the opportunity to provide the committee with an overview on the state of adoption of Radio Frequency Identification (RFID) in the retail sector.

By way of background, The Retail Industry Leaders Association (RILA) is an alliance of the world's most successful and innovative retailer and supplier companies—the leaders of the retail industry. RILA members represent more than \$1 trillion in sales annually and operate more than 100,000 stores, manufacturing facilities and distribution centers nationwide. Its member retailers and suppliers have facilities in all 50 states, as well as internationally, and employ millions of workers domestically and worldwide. Through RILA, leaders in the critical disciplines of the retail industry work together to improve their businesses and the industry as a whole. The mission of RILA is to lead and serve the most successful and innovative retailers and suppliers through the delivery of world-class education, innovation and advocacy.

The promise of RFID is nothing less than revolutionary for the retail and supplier community. While RF technology has been used for decades, the retail and supplier communities are beginning to implement RFID as a new tool in supply chain management and distribution. Global supply chain total annual spending is a staggering \$3 trillion. Total estimated annual loss due to poor supply chain visibility is estimated between six and 10 percent—an annual loss of \$180–\$300 billion.

RFID offers significant benefits to the retailer and supplier community as well as their customers. Providing retailers with continuous access to the location of merchandise in the supply chain, RFID will allow them distribute merchandise more efficiently, reduce costs associated with holding large inventories, or “safety stock,” increase sales through reduced out of stocks, and allow for more accurate forecasts and stock replenishments. The application of RFID in the supply chain could reduce transportation costs and shipping volumes and increase stock visibility and availability at the point of shipment. In addition, RFID can help curb theft and “shrink” in the supply chain.

The supply chain applications for RFID also hold important customer benefits including better in-store stock—the products customers want on the shelf when they want them. More efficient inventory management will lead to improved product selection, product freshness for dated goods, and easier identification on recalls. In short, RFID will help retailers get product to their stores in a more effective manner ensuring that consumers have access to a wide range of merchandise when and where they want it.

RFID deployment by the retail industry is still very much in its infancy. As a whole, the industry is in a discovery and exploratory mode focusing on supply chain applications. A number of retailers and suppliers are engaged in RFID test pilot initiatives, and are focused predominately on RFID tagging at the case and pallet level to increase supply chain efficiencies. Implementation of RFID at any level is an extremely high-cost proposition. While much of the RFID discussion has focused on the item-level tagging of consumer products, most industry experts and market analysts agree that wide spread item-level RFID tagging is a decade or more in the future. In fact, the proposition is so costly that a leading technology firm does not foresee widespread tagging of individual items costing less than \$10 until 2017 at the earliest.

While widespread item-level tagging is years in the future, much of the focus on RFID implementation at the retail has been related to tagging individual consumer product. RILA members view RFID technology is the next generation of the bar code and like the bar code RFID tags contain product information, not customer information. It is new product management devices that can more efficiently track inventory and product throughout the retail supply chain.

RILA is working actively to maintain a public policy environment that will foster innovation and adoption of RFID technology and ensure that retail and supplier applications are allowed to mature. While some have suggested that new laws, RILA members believe legislation in this area would be premature and would unnecessarily stifle innovation and deployment. Retailers are focused on enhancing the cus-

tomers' in-store experience. They spend millions of dollars each year to make their stores more inviting to the consumer and to enhancing customer loyalty. Retailers recognize that customers vote with their feet everyday and are committed to implementing RFID technology in a way that respects our customers, provides added value and enhances the shopping experience.

