"HOW DO BUSINESSES USE CUSTOMER INFORMATION: IS THE CUSTOMER'S PRIVACY PROTECTED?"

HEARING

BEFORE THE

SUBCOMMITTEE ON
COMMERCE, TRADE, AND CONSUMER PROTECTION

OF THE

COMMITTEE ON ENERGY AND
COMMERCE
HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTH CONGRESS

FIRST SESSION

JULY 26, 2001

Serial No. 107–49

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

74–846CC WASHINGTON : 2001

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

W.J. "BILLY" TAUZIN, Louisiana, *Chairman*

MICHAEL BILIRAKIS, Florida
JOE BARTON, Texas
FRED UPTON, Michigan
CLIFF STEARNS, Florida
PAUL E. GILLMOR, Ohio
JAMES C. GREENWOOD, Pennsylvania
CHRISTOPHER COX, California
NATHAN DEAL, Georgia
STEVE LARGENT, Oklahoma
RICHARD BURR, North Carolina
ED WHITFIELD, Kentucky
GREG GANSKE, Iowa
CHARLIE NORWOOD, Georgia
BARBARA CUBIN, Wyoming
JOHN SHIMKUS, Illinois
HEATHER WILSON, New Mexico
JOHN B. SHADEGG, Arizona
CHARLES "CHIP" PICKERING, Mississippi
VITO FOSSELLA, New York
ROY BLUNT, Missouri
TOM DAVIS, Virginia
ED BRYANT, Tennessee
ROBERT L. EHRLICH, Jr., Maryland
STEVE BUYER, Indiana
GEORGE RADANOVICH, California
CHARLES F. BASS, New Hampshire
JOSEPH R. PITTS, Pennsylvania
MARY BONO, California
GREG WALDEN, Oregon
LEE TERRY, Nebraska

JOHN D. DINGELL, Michigan
HENRY A. WAXMAN, California
EDWARD J. MARKEY, Massachusetts
RALPH M. HALL, Texas
RICK BOUCHER, Virginia
EDOLPHUS TOWNS, New York
FRANK PALLONE, Jr., New Jersey
SHERROD BROWN, Ohio
BART GORDON, Tennessee
PETER DEUTSCH, Florida
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
BART STUPAK, Michigan
ELIOT L. ENGEL, New York
TOM SAWYER, Ohio
ALBERT R. WYNN, Maryland
GENE GREEN, Texas
KAREN MCCARTHY, Missouri
TED STRICKLAND, Ohio
DIANA DEGETTE, Colorado
THOMAS M. BARRETT, Wisconsin
BILL LUTHER, Minnesota
LOIS CAPPS, California
MICHAEL F. DOYLE, Pennsylvania
CHRISTOPHER JOHN, Louisiana
JANE HARMAN, California

DAVID V. MARVENTANO, *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*

NATHAN DEAL, Georgia
Vice Chairman
ED WHITFIELD, Kentucky
BARBARA CUBIN, Wyoming
JOHN SHIMKUS, Illinois
JOHN B. SHADEGG, Arizona
ED BRYANT, Tennessee
STEVE BUYER, Indiana
GEORGE RADANOVICH, California
CHARLES F. BASS, New Hampshire
JOSEPH R. PITTS, Pennsylvania
GREG WALDEN, Oregon
LEE TERRY, Nebraska
W.J. "BILLY" TAUZIN, Louisiana
(Ex Officio)

EDOLPHUS TOWNS, New York
DIANA DEGETTE, Colorado
LOIS CAPPS, California
MICHAEL F. DOYLE, Pennsylvania
CHRISTOPHER JOHN, Louisiana
JANE HARMAN, California
HENRY A. WAXMAN, California
EDWARD J. MARKEY, Massachusetts
BART GORDON, Tennessee
PETER DEUTSCH, Florida
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
JOHN D. DINGELL, Michigan,
(Ex Officio)

CONTENTS

"HOW DO BUSINESSES USE CUSTOMER INFORMATION: IS THE CUSTOMER'S PRIVACY PROTECTED?"

THURSDAY, JULY 26, 2001

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

The subcommittee met, pursuant to notice, at 9:35 a.m., in room 2322, Rayburn House Office Building, Hon. Cliff Stearns (chairman) presiding.

Members present: Representatives Stearns, Shimkus, Bryant, Walden, Terry, Bass, Tauzin (ex officio), Towns, DeGette, Doyle, John, and Harman.

Staff present: Ramsen Betfarhad, majority counsel; Michael O'Reilly, professional staff member; Brendan Williams, legislative clerk; and M. Bruce Gwinn, minority counsel.

Mr. STEARNS. Good morning, good morning. I welcome all of you here. This is the sixth and last in a series of hearings on information privacy held by our Subcommittee on Commerce, Trade, and Consumer Protection. This hearing concludes one phase of the subcommittee's inquiry into information privacy, but not the inquiry itself.

I think these hearings have fulfilled their objective of informing members and the public at large, in a deliberate and careful manner, of the many issues implicated by the privacy debate. The collective record of the six hearings is a rich resource of information and opinion on the issue of information privacy, and should be used to inform all of us on the debate on this issue.

I commend members of the committee to review the hearings that we have had, the record that has been amassed by this subcommittee on this important issue of information privacy, before they seek to formulate or finalize their judgments on this matter. In no other location, either within or without the Hill, will we find a more comprehensive record on information privacy.

I am especially pleased to have as witnesses executives that represent some of the most revered companies in corporate America. We all are or have been, at one time or another, customers of General Motors, IBM, Proctor & Gamble, Amazon.com, and Land's End. I appreciate the fact that these companies didn't have to be here testifying on the difficult public policy matter of information

privacy. So I recommend—I commend all of them for their participation and wish to thank them for coming.

Many have written on or spoken to the issue of information privacy in the commercial world, as if the issue existed in a vacuum. That is to say, some commentators on information privacy speak with little or no consideration of the realities that characterize the intersection between privacy and the commercial world. Today, we have the rare opportunity to ask these large transnational corporations, representing differing industries, and the three top compilers, what really transpires in the real world with respect to consumer information.

The witnesses on the first panel represent a diverse group of companies, ranging from the world's largest industrial corporation with 400,000 employees, to one that markets 300 brands of consumer products to nearly 5 billion customers—let me repeat, 5 billion customers—worldwide, and an online company that in less than 6 years has become one of the most recognized brands in retailing. These companies will all speak to how they collect customer information; what types of information they collect; what uses they put that collected information to; why they use the information in the way that they do; and what business or legal incentives are in place assuring the proper utilization of that consumer information.

Moreover, the witnesses on the second panel, representing data compilers, will help us better understand what it is that they do. We may know the most about the credit reporting services. We have, all of us, invariably been subjected to credit checks in the course of our ordinary lives, when applying for a car loan, a mortgage, credit cards, et cetera. Yet many of us may not know that these three companies provide authentication and verification services enabling the seamless and speedy execution of millions of small and mundane transactions every day, such as the purchase of a CD online from Amazon.com or off-line from Tower Records.

The insight offered by our witnesses is especially important when considering the fine balance present between the proper and improper collection and use of consumer data. As these hearings have established, there are substantial benefits that accrue to our economy from the unencumbered flow of information, particularly consumer information. Meanwhile, these same hearings have highlighted the fact that Americans do have concerns regarding abuses that may arise from the collection and/or use of certain types of consumer information in the commercial context.

The objective today, in this hearing, is to demystify—make concrete—data collection and use practices common in the commercial world today. To put it more bluntly, the testimony, I hope, will help separate fact from fiction, reality from myth, when it comes to the issue of information privacy. Only when empowered with real facts can Congress advance good public policy addressing information privacy.

So, Mr. John, you are welcome with an opening statement.

Mr. JOHN. Yes, thank you, Chairman Stearns. My friend and colleague, the ranking member from New York, is tied up at this moment in another subcommittee, on Commerce and Health. And I temporarily will try to fill his large shoes. Me being from Louisiana

and him from New York, those are very big and different shoes to fill.

But I ask unanimous consent that all members be permitted to include their statements into the record.

Mr. STEARNS. By unanimous consent, so ordered.

Mr. JOHN. Thank you.

I am sure that the panelists are ready to get started. I want to thank them and welcome them, the first panel and also the second panel, and express my really sincere thanks to Chairman Stearns for having a series—the sixth, as he said—on issues that are very important on information privacy.

I also believe that these hearings have been useful, and helpful, and they have meant a lot because of the issues that are confronting businesses, regulators, and consumers. And I really look forward to hearing from the folks that deal with this issue every day, and working with the chairman and the ranking member as we move through this process legislatively.

So, welcome. And I look forward to hearing your testimony. Thanks.

Mr. STEARNS. I thank the gentleman. The gentleman from Illinois, Mr. Shimkus?

Mr. SHIMKUS. Thank you, Mr. Chairman. I, too, want to welcome the panel. I would have walked over and introduce myself; I was here early. But I have an athletic injury, that I am doing as little walking as possible. But we do appreciate your attendance.

We have dealt with, are trying to understand this from the public policy position. Of course, many of us were with the Commerce Committee when we passed Graham-Leach-Bliley. But statements have constantly been made in this committee that we want to get a handle on how privacy is good for business—obviously, that is what we hope to hear from you all today—and how you go about doing that.

In the financial services arena, there is some argument about how sharing of information within a designed arena is actually good for some consumers, too. And that may not be true in your business. So that is why this panel is unique in some of the discussions we have had. I look to focus on that area. I appreciate your expertise and your willingness to come before us.

And with that, Mr. Chairman, I yield back my time.

Mr. STEARNS. The gentleman yields back. Mr. Doyle, the gentleman from Pennsylvania?

Mr. DOYLE. Thank you, Mr. Chairman. I just want to welcome our panelists this morning. I think we're all anxious to hear what they have to say. And I will ask unanimous consent that my statement may be made part of the record, so that we can hear our panelists. And I yield back.

[The prepared statement of Hon. Mike Doyle follows:]

PREPARED STATEMENT OF HON. MIKE DOYLE, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF PENNSYLVANIA

Thank you Mr. Chairman and Ranking Member, for holding this hearing. I am looking forward to learning about the technologies, policies, and approaches that some of the leaders in the electronic commerce industry have employed to prevent unwanted dissemination and use of our private consumer information. Thank you all for taking the time testify this morning.

As the discussions regarding individual consumer privacy progress in America and before this subcommittee, I know think many of my constituents back in the Pittsburgh area are not just asking "how do business use my information" but they are saying, "wait a minute, you mean businesses have been gathering my personal information all along?"

I often find that consumers in Western Pennsylvania seem to have no problem allowing certain personal information to be collected and used by industry. For example, the regional supermarket, Giant Eagle, asks for certain access to personal shopping information through the use of the Giant Eagle Advantage Card. I myself use such a card.

It provides incentives that members undoubtedly find useful, such as discount coupons through the mail for items that a customer routinely purchases. Obviously, this is an example of personal information use that both client and consumer find beneficial and acceptable.

Protecting this type of personal information, while important, is decidedly different than protecting against abuses associated Social Security numbers, birth dates, mother's maiden names, or health records. It is the extent to which this personally identifiable information is collected, used, and distributed that pose the greatest threat to true privacy and create the need for Congress to find a solution to protect consumers.

The industries represented this morning by our esteemed panelists are some of the most successful and profitable companies in America. I am anxious to hear of the problems associated with implementing their effective self-regulatory policies, for if our Fortune 100 companies have difficulty funding privacy protection policies, surely our smaller firms or medium size companies will have greater problems generating the necessary capital and resources.

In closing, Mr. Chairman, I look forward to finding a way that Congress can augment and aid effective industry self-regulation in a manner that will not impede the continued development of e-commerce, while protecting and ensuring consumer rights are upheld.

Mr. STEARNS. The gentleman yields back. His opening statement will be made a part of the record.

And the gentleman from New Hampshire, Mr. Bass?

Mr. BASS. Thank you very much, Mr. Chairman. And I, too, join my colleagues in thanking you for having this final hearing. It has been a fascinating series of hearings. I have learned more, I think—learned a lot more than I have been able to impart to other folks about this issue, which is extremely complex.

And I hope that we will be able to clear up some of the misconceptions that may exist about corporate or business use of personal information vis-a-vis Internet transactions. And I also hope, Mr. Chairman, that as we listen to these witnesses, we try to separate what may already be illegal anyway under existing law from what may need to be attended to by the Congress.

And we may not need to do anything. But again, I think it is important that this committee fully and thoroughly investigate the issue so that we understand, so that we understand its complexity and scope, so that as the Internet becomes more and more significant in the economy—not that it isn't already—that we will be in a position to deal with it from a position of strength, rather than ignorance.

And I appreciate the chairman holding these hearings.

Mr. STEARNS. I thank the gentleman.

[Additional statements submitted for the record follow:]

PREPARED STATEMENT OF HON. W.J. "BILLY" TAUZIN, CHAIRMAN, COMMITTEE ON ENERGY AND COMMERCE

Thank you, Mr. Chairman for calling this hearing. I understand that this will conclude the series of education hearings you have held on privacy, so I also want to commend you for developing a process that allows us to consider this issue in a thoughtful and deliberative manner.

The topic of today's hearing is very important in the overall privacy debate. Too often in Washington we are told how it works in the real world through the eyes of Washington-based trade associations, lobbyists and consumer groups. Today's witnesses will provide a different perspective—from the real world. I appreciate their willingness to come forward and share their knowledge and experience.

As Chairman of the Committee, and as a consumer, I have heard and seen a great deal of activity by American companies. Let me sum up what they tell me: they like to exploit consumers for all their worth, they know consumers don't care about product quality, they don't try to maintain good customer relations, they can always find new customers to replace dissatisfied customers, they don't think that their brand name is that important, and they don't care about consumer privacy. I joke for purposes of making a point—*Companies Do Care About Consumer Relations.* The litany of untruths I just rattled off is completely opposite from what I have experienced from American business.

In our market economy, competition compels companies to strive to meet consumer needs. If a company doesn't do what customers want, they'll go elsewhere. People sometimes seem to forget this. Yet, it is a fundamental fact of commerce that service to the consumer is the cornerstone of a successful company.

Privacy is becoming a factor that consumers take into account as they shop. It may not be the primary concern, but it is a factor. Many companies have recognized this and have responded in kind with improved privacy practices. In fact, many of the privacy requirements that some want mandated by Washington are already being implemented by reputable companies. It is simply sound business practice to do so.

Some companies even use their privacy practices to gain competitive marketing advantage over competitors. IBM, for instance, recently plastered a picture of their privacy guru, who is here with us today, in countless advertisements. Obviously, they see a positive side to the privacy debate.

So, it is instructive to examine just how real companies are dealing with privacy in the real world. We need to learn how established leaders in the American economy (and often the trend-setters) collect customer information, what the information is used for, and how companies handle consumer privacy. I hope the panelists will enlighten us on these points.

I also hope that this hearing will help debunk the scary scenarios that have been created to stir up consumer angst. Over the past few years, we have heard a lot of crazy stories about how consumer information is used. Many of these stories have proved to be false.

Furthermore, I am pleased to see a discussion of the practices of the so-called data aggregators. Most people have had experience with the credit ratings services of some of these companies, but they often offer many other services. It is important to demystify just how they operate and what they do.

I note that one of the benefits of data aggregators is of direct benefit to consumer needs—the reduction of junk mail. If you have ever received a catalog addressed to you that you have completely no interest in then you know firsthand the results of poor information. The accurate information provided by aggregators helps companies offer consumers the products and services they will find useful. Of course, many people have questioned the privacy practices of data aggregators and so here is a chance to set the record straight.

Going forward, one thing should be clear: I don't see a need to legislate on false scenarios. We cannot and will not design some elaborate new privacy regime that will take into account every possible daydream of how information *could* be used. Reality must be taken into account. We will look to all parties to keep this in mind as we proceed in this debate.

I thank the Chairman and appreciate his indulgence.

PREPARED STATEMENT OF HON. EDOLPHUS TOWNS, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NEW YORK

Thank you Mr. Chairman and I too would like to welcome the witnesses to our sixth hearing on Privacy.

Nearly every company across the country compiles information on the consumers who use their products and some companies compile the data to sell to other corporations. I am interested to hear what the companies assembled here today have to say regarding their handling of personal information.

Consumers across the country are literally begging to be informed on how their information is collected, used and PROTECTED. And that is assuming they realize who is collecting the information.

It is my hope today that the witnesses will shed light on not only their practices on HOW they collect information, but what they do with it after they get that information.

I would like to commend the witnesses today. They have chosen to step forward and educate members of the committee on this topic. You all have invested in making consumer's privacy a priority.

This brings me to the main reason I am advocating some sort of minimum privacy standards. Not all companies are doing what Fortune 100 companies do. Not all of them take their customer's as seriously as do others.

As I weigh this issue over the August recess and decide what type of privacy bill to submit, consumer and corporate responsibility will serve as my compass and I look forward to reviewing the testimony of past witnesses and hearing the testimony of those assembled here today.

Mr. Chairman, with that I yield back the balance of my time.

PREPARED STATEMENT OF HON. JOHN D. DINGELL, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF MICHIGAN

Mr. Chairman, I want to thank you for holding this important hearing. Privacy has been a major consumer concern for a long time, and that concern has increased greatly with the advent of the internet and e-commerce. In fact, market researchers estimated last year that consumer concerns about privacy and security caused e-retailers to lose $6.1 billion in sales worldwide. Clearly, business is paying a big price for the concerns consumers continue to have about online transactions.

For some online businesses, strong privacy protections have become the key to greater competitiveness in the marketplace. Many firms now highly publicize their privacy policies as they vie with each other to see who can give consumers the greater comfort and security about online retailing. Today we will hear from several large businesses that have heard and responded to the privacy concerns of consumers.

While I compliment these companies for their initiative and responsibility, I would caution my colleagues against drawing any conclusion that what these firms have done is representative of all business. It is not. And it is because it is not that the Federal Trade Commission (FTC) has recommended that Congress pass online privacy legislation.

The FTC reported to Congress last year, and I quote, "only 20% of the busiest sites on the World Wide Web implement to some extent all four fair information practices in the privacy disclosures." The FTC goes on to say, "Moreover, the enforcement mechanism so crucial to the success and credibility of self-regulation is absent."

Mr. Chairman, a privacy right that is not enforceable is not worth the paper it's written on, or in this case the screen. That is why this Subcommittee needs to complete these hearings and get about the important task of considering legislation. The legislation needs to establish minimum standards governing the handling of information online. It needs to give the FTC authority to promulgate more detailed standards as necessary. And most importantly, it needs to provide adequate enforcement authority. Without an effective means of enforcing consumer privacy rights, consumers have no way to guarantee their rights are protected.

Mr. Chairman, again I thank you for holding this hearing, and I look forward to working with you and the Ranking Member of the Subcommittee, Mr. Towns, on legislation to make sure that the privacy rights of consumers that engage in online transactions are fully protected.

Mr. STEARNS. And now we will have our first panel. Let me welcome all of you. Ms. Harriet Pearson, Chief Privacy Officer from IBM; Ms. Jacqueline Hourigan, Director of Corporation Data Policies, General Motors Corporation; Mr. Zeke Swift, Director, Global Privacy, Proctor & Gamble; Mr. Paul Misener, Vice President, Global Public Policy, Amazon.com; and Mr. David Johnson, Vice President, Direct Marketing, Land's End, Incorporated.

I welcome you. And Ms. Pearson, we will have your opening statement.

STATEMENTS OF HARRIET P. PEARSON, CHIEF PRIVACY OFFICER, IBM; JACQUELINE L. HOURIGAN, DIRECTOR, CORPORATION DATA POLICIES, GENERAL MOTORS CORPORATION; ZEKE SWIFT, DIRECTOR, GLOBAL PRIVACY, PROCTER & GAMBLE; PAUL MISENER, VICE PRESIDENT, GLOBAL PUBLIC POLICY, AMAZON.COM; AND DAVID A. JOHNSON, VICE PRESIDENT, DIRECT MARKETING, LAND'S END, INC.

Ms. PEARSON. Thank you, Mr. Chairman. And members of the committee, thank you for inviting IBM to share our views on this important subject.

My name is Harriet Pearson. I am the Chief Privacy Officer for IBM. We are the world's largest information technology company, and the world's largest e-business services company. We believe that from that vantage point we have a unique perspective on the issue of privacy, dealing as we do with so many customers who use information in their own businesses worldwide.

IBM has a longstanding commitment to privacy dating back to the 1960's. We were among the first corporations to develop a global privacy policy, focusing first on our employees. We were the first online advertiser to advertise and restrict our advertising only to those Internet sites that posted privacy policies. We are a leader in privacy and security technologies, with over 600 patents in that area.

As Chief Privacy Officer, I manage our internal privacy policies, help bring together our research and technology initiatives, and engage customers and policymakers worldwide on this issue. The effort is complex for a large company like ours. For example, on the web, ibm.com has over a million pages of content, and each site needs to have a privacy statement. Privacy is a priority for IBM, and for the health of our marketplace.

With that introduction, I would like first to comment upon how we use data ourselves, since that is a topic of this hearing. Then second, I would like to provide some observations from where we sit on how others, thousands of our customers, use data for their processes. And finally, I would like to close with several recommendations for how you as policymakers can continue building a record in this area and further the public policy agenda.

I would like to turn to IBM first. The primary subject of this hearing is how companies use data. We at IBM strive to use data creatively and responsibly. Most of IBM's customers are organizations rather than individuals, but in both cases we use data to identify likely customers, understand their needs, and to market to them. We use data to offer the right solutions, deliver orders efficiently, offer strong service and support, and to maintain good relationships.

These normal business functions require the collection and effective use of data about individuals. For example, when a consumer purchases an IBM personal computer, whether it is an Aptiva or a ThinkPad, we use information about their purchase, such as their name, address, phone, e-mail address. And we collect their preferences about whether or not they wish to be contacted. If they choose to register with what we call our Owner Privileges program, we use their information to provide a free product update news-

letter, prioritize telephone handling with a special toll-free number, and other special offers.

We govern our use of information with corporate-wide policies and practices on privacy. They govern how we use information worldwide. These policies require us, globally, to provide individuals notice of our information practices, and of the choices they can make about the use of their data. We require, also, ourselves to implement appropriate security and accuracy measures. And finally, we also have contractual protections for customers when we share data with our business partners and suppliers. And we do share data with those suppliers and business partners; lots of companies help us go to market and do business.

IBM is leading within the larger business trend of becoming accountable on privacy. From our vantage point, working as we have with nearly 20,000 businesses in the last several years implementing and using the Internet to improve their businesses, we see firsthand how they use information to improve, in turn, their services and products for their consumers. These companies use consumer information in ways very similar to those I have just stated. And my experience is, personally and my colleagues', is that they have the same level of concern for consumer satisfaction and privacy.

For example, one of our grocery chain customers uses information about consumer purchases to improve their decisions about which items to stock and when; to offer discounts; and to tailor promotions to individual customers. Data helps them reduce costs, and to run their company more efficiently, and to provide better service for their consumers.

I have mentioned other examples in my written statement, and you will of course hear from the other companies here today. I personally have spoken with 100 or more, hundreds, of companies in the first 6 months of this year, and I can see significant growth in awareness of privacy issues, and a commitment to doing the right thing with respect to consumers. It is amazing to see how the level of awareness has grown within the U.S. business community.

I believe the heart of the privacy challenge is that individuals must understand how information about them is used and how they benefit. They should be able to exercise choices and feel that the system that handles their information is under control. They need to feel confident that the relationships in which they enter are going to be ones that respect their wishes.

It is important that we focus on these issues now and later. From our vantage point, it is clear that we are still in the early stages of a technological revolution that will change how we as businesses deal with consumers, and it is only going to keep accelerating in terms of how the technology lets us manage information. Therefore, I conclude with a few thoughts on how you as policymakers can move ahead.

The point, it seems to me, is to find a balanced approach between government regulation, industry action, and individual responsibility. And our view is that a framework for those issues and how to approach it has emerged in this country. It is built on top of over 30 existing laws on privacy; layered on top of that, industry initiatives and proactive engagements by companies such as ours; and

on top of that, the kinds of tools and technologies that are available now for companies to use.

We need to have a deliberative approach, as you, Mr. Chairman, and the members of the committee have agreed to, to study these issues and find out, where is the harm? Where are the issues that need to be addressed? And how public policy fits into that picture. I commend you for your approach. We at IBM would like to continue to be a constructive player in this process. And we thank you for the opportunity to share our views.

[The prepared statement of Harriet P. Pearson follows:]

PREPARED STATEMENT OF HARRIET P. PEARSON, CHIEF PRIVACY OFFICER, IBM CORPORATION

Thank you Mr. Chairman for inviting me to share IBM's views.

My name is Harriet Pearson and I am the Chief Privacy Officer of the IBM Corporation. IBM is the largest information technology company in the world. We develop and manufacture many of industry's most advanced technologies, including computer systems, software, networking systems, storage devices and microelectronics. We also are the world's largest e-business services company, delivering strategic consulting and helping our clients to use information technology to improve their internal operations and service to customers. This gives us a unique vantage point from which to comment on privacy issues, working as we do on a global basis with companies, governments, and organizations of all sizes.

IBM has a long standing commitment to privacy. In the 1960s, IBM developed one of the first global privacy approaches for business, focused around employee privacy. As the computer revolution progressed, we supported privacy legislation to protect e-mail and medical information. IBM remains a leader in privacy and security technology—currently holding over 600 patents for such technologies. IBM was the first online advertiser to announce that it would only advertise on Internet sites that posted privacy policies. Last year our CEO, Louis Gerstner, appointed me as IBM's Chief Privacy Officer to confirm that IBM has the right internal policies in place, to help unify our many privacy research and technology initiatives, and to engage customers and policymakers worldwide about privacy issues.

I'm certainly not alone at IBM in my efforts. We have a privacy team that works across IBM in areas like marketing, development, services, human resources, and legal. The effort is complex for large companies. IBM is an $88 billion company that employs more than 300,000 people in the United States and operates in 160 countries. On the Web, ibm.com has more than a million pages of content and each site needs to have a privacy statement.

Externally, IBM's Privacy Consulting and Technology teams are helping organizations implement sound privacy practices and giving them the tools to do so. At all levels, IBMers speak out about the importance of privacy and are backing their words with actions to help build a responsible marketplace that can earn people's trust. In short, privacy is a priority within IBM and it is important to the health of the marketplace in which we operate.

HOW IBM USES CUSTOMER DATA

IBM policies and practices are designed to let us use data creatively and responsibly. Most of IBM's customers are corporate rather than individual clients. In both situations we work to identify likely customers, understand their needs, and market to them. We strive to offer the right solutions, deliver orders efficiently, offer strong service and support, and maintain good relationships in hopes of earning future sales. All of these normal business functions require the collection and effective use of data about individuals.

For example, when an individual or small business owner purchases an IBM Aptiva or Thinkpad personal computer, we ask them for information about their purchase, their name, address, phone, e-mail and preferences about being contacted. As a special service for those customers willing to take the time to register with our Owner Privileges program, we use this information to provide a free e-mail newsletter, prioritized telephone handling through a special toll-free number, and special offers for registered customers (e.g. coupon for free stamps from Stamps.com).

We inform customers about their choices not to receive further marketing materials from IBM, and respect their preferences. We might also use third-party sources

like the National Change of Address Service managed by the U.S. Postal Service to verify address changes. We thus use customer information to provide better and more-tailored service, while solidifying the relationship with the customer.

The net result? In this and other situations involving customer information, IBM is able to offer services better-targeted to those who might be interested, while at the same time delivering fewer solicitations to people who are not.

IBM has a set of corporate-wide policies and practices to govern our actions when we use personally identifiable data and we train IBM professionals who are bound by these policies and practices. Our policies also require that we put in place contractual protections when we share data with business partners and suppliers.

When IBM gathers personally identifiable information online, we offer notice of our privacy practices and inform the individual of their choices regarding the use of that data. In the case of e-mail solicitations, IBM requires that the individual first give his or her permission before the e-mail is sent unless we already have an existing business relationship. Our policies require that we safeguard the information in our possession and limit its visibility.

IBM is leading within a larger business trend of taking action to be accountable on privacy. In just the past few years, we've seen a rapid growth of the number of online privacy statements, chief privacy officers, privacy technologies, seal programs, and in the U.S., targeted laws to protect sensitive information. This subcommittee should be proud its work to explore what further needs to be done. To best reap the benefits of the information economy and preserve privacy in the process, there must be a balanced approach. IBM believes it should begin with an understanding of what the future holds.

THE FUTURE OF THE INFORMATION ECONOMY

Much has been said about the demise of the information economy in the wake of the dot.com meltdown. In fact, however, we are still in the early stages of a global technological transformation that will revolutionize our society over the next 25 years, driving our economy and exponentially expanding our opportunities. The transformation is being fueled by the rapidly increasing power of the technology itself and of information networks. These enable new models for business, health care, education and government.

The Internet will transform every important business transaction and relationship. This includes improving relations with customers, but much more. It also means transforming relations with people who want to invest with you and people who want to work for you. Companies also will use the Net to integrate supply chains that connect an enterprise to markets and industries. Internal transactions, such as order processing, fulfillment, logistics, manufacturing and employee processes, will be faster and less costly.

Companies will even be able to be in contact with their products—appliances, industrial machinery, consumer electronics—so the company can provide after-sale service, understand product performance, and make improvements. Government will evolve similarly, as taxpayers will expect not only online services, but also efficient management. The benefit is very significant in hard dollar savings and cost avoidance when transactions are performed on the Web as opposed to the old paper format. For example, IBM saves 70 percent on transaction costs when we use the Web and we have seen many similar results across industry as a result of e-transformations.

However, all this adds up to massive data collection and management and requires a heightened awareness and commitment to privacy throughout our society.

My colleagues and I at IBM see first-hand how thousands of companies use information to improve *their* service and products for consumers—we've helped over 18,000 businesses successfully leverage the Internet. And these companies use consumer information in ways very similar to the companies at today's hearing, and with much the same level of concern for consumer satisfaction and privacy.

Here are some examples:

- A multi-billion dollar US-based financial services firm uses state-of-the-art database technology in a way that's allowed them to anticipate customer needs and to respond rapidly. The company uses customer information to help it pinpoint delinquencies early, so it can work harder and earlier with customers to help them become solvent again. It can better tailor product offers to those who might be interested—for example, offering coupons toward phone service for those customers who achieve a certain level of usage. The firm's objective is to treat all of its customers with the same level of respect and to discover what is important to each customer.

- A utility company uses the consumer information it collects to identify customers that may be interested in additional services and market them accurately; to further customize rates and offer analysis to specific customers; to generate personalized reporting much faster than it was able to previously; and to diversify their service offerings and react quickly to new business opportunities.
- A grocery store chain uses information about consumer product purchases to: make better decisions about which items to stock and when; to offer customized discounts and other offers on those products which an individual customer buys or may be likely to be interested in; and overall to reduce cost and run the company more efficiently.

It is clear that the fullest fruits of the information revolution will remain untapped unless individuals can understand how information about them is collected and communicated to others. This lack of knowledge can drive feelings of mistrust, fear, and a loss of control. Individuals also must understand that they benefit from information exchanges in terms of savings, convenience, services, and jobs. Many surveys show that people want products quickly and conveniently and want high levels of service. They realize that some information exchange is needed.

Importantly, individuals must be able to exercise choices and feel that the system is under control. They must feel confident entering into data sharing relationships with banks, doctors, credit card companies, grocery stores and their government. This is the heart of the privacy challenge.

NEED FOR A BROADER U.S. PRIVACY DEBATE

Agreement is emerging around the world that private sector initiatives are critical to address privacy concerns in day-to-day commercial activities. Even in environments that embrace strict data processing regimes like the European Union, governments recognize that robust and accountable market-led measures must play a prominent, if not preeminent, role. Europeans call it "co-regulation." In the United States it is often referred to as industry self-regulation.

Business leadership is crucial because governments do not have the manpower, technology, or jurisdictional authority to comprehensively monitor consumer transactions in cyberspace, nor would many people *want* government to carry out such a task if it could. This brings me back to the question I posed earlier about preserving privacy *and* the benefits of the information economy: Is there a balanced approach between government regulation, industry action, and individual responsibility?

As this subcommittee established at an earlier hearing, approximately 30 federal laws regulate privacy in some form. These laws tend to focus on (1) preventing fraudulent or harmful uses of data (e.g. identity theft, employment discrimination, deceptive trade practices, or surreptitious monitoring of e-mail) and (2) establishing special rules and protections for sensitive information (e.g. financial, medical, and children's data).

Layered upon these protections are industry initiatives like privacy policies, seal programs, industry codes of conduct, and suppression lists for telemarketing and commercial e-mail. Furthermore, people can use privacy technologies to control cookies or to surf, shop, and send e-mail anonymously. Many are free and some are being built into the architecture of the online marketplace (e.g. the Platform for Privacy Preferences).

U.S. law and practice reflect a desire to balance individual privacy and the societal benefits of data availability (e.g., economic efficiency, free speech, accountable government). This is a solid framework and should be the basis on which any new or modified U.S. privacy regime is built.

Some have asked, "where is the harm" in data collection as a rhetorical question to imply there is no harm or risk. We should ask the question in earnest. And then answer it by devising responses to people's real and legitimate concerns about data, such as identity theft, financial fraud, disclosure of embarrassing information, employment discrimination, denial of insurance, government seizure, or nuisance issues like spam. We should not create laws because of a vague notion that data collection itself is harmful.

We need to examine the incidence of these concerns, identify their causes, assess any harm they may cause, and then as leaders—in government and the private sector—ensure that an appropriate policy regime is in place. Too much of the privacy debate now speculates on how commercial data *might* be used without going through these steps. We should identify a spectrum of privacy concerns and link them with protections afforded by current law and practice. Most Americans are unaware of the privacy protections afforded them now by the Fair Credit Reporting

Act, the FTC Act, the Network Advertising Initiative, the Privacy Act, the Electronic Communications Privacy Act, and the Fourth Amendment.

Against this backdrop we should review proposals by Members of Congress and consider what further actions might be appropriate for industry or the Administration. This subcommittee has demonstrated that privacy has many dimensions and is complex, but I sense that we are beginning to gain a fuller knowledge and perspective that will allow us enter a more productive dialogue on privacy and to craft appropriate responses.

In summary, we should build on current law where necessary and link solutions to people's top priorities. We appreciate the subcommittee's thoughtful examination of privacy issues and the critical role you will play in shaping balanced, appropriate responses. IBM is committed to continue being a constructive player in this process. For example, we have joined with other companies in groups such as the Privacy Leadership Initiative to further the contributions that the private sector can make to understanding these complex issues and communicating helpful information to fellow business and consumers.

Most companies agree that any U.S. privacy regime should be a national solution, not a patchwork of fifty conflicting regimes. The regime should encourage transparency and choice. It should hold government and non-profit organizations accountable to similar standards asked of industry. It should neither discriminate against the Internet nor create new private rights of action.

In consummary, IBM believes that the best privacy model is a layered approach of responsible industry action, consumer-empowering technology, and targeted government action that promotes transparency, protects sensitive information, and appropriately addresses harmful and fraudulent data practices. This framework can build consumer trust and remain flexible enough to allow companies to offer the convenience, savings, services, and jobs that benefit our citizens.

Thank you for this opportunity to share our views.

Mr. STEARNS. Thank you.

Ms. Hourigan?

STATEMENT OF JACQUELINE L. HOURIGAN

Ms. HOURIGAN. Good morning, Mr. Chairman and members of the subcommittee. My name is Jacqueline Hourigan, and I am the Director of Corporate Data Policies for the General Motors Corporation. I welcome the opportunity to appear today to discuss GM's perspectives of this very complex issue of data privacy.

As you heard earlier, we have over 400,000 employees, 30,000 suppliers, and 8.7 million vehicles sold last year in over 200 countries. As a result, the collection, use, and security of personally identifiable data, collected both on the Internet and in the off-line world, are critically important issues for GM. As a result, we do appreciate the deliberative and thoughtful approach this committee has taken to this incredibly complex issue.

Our customers' trust is a priority for GM, and we are working to balance our customers' needs and expectations with the benefits available from the free flow of information. Specifically, we seek to align our internal policies and processes with customer expectations and data privacy laws worldwide.

We collect information through a variety of means, including standard market research and response techniques; visits to GM web sites; product purchase channels; as well as in-vehicle technology designed to enhance the safety and security of our drivers on the road.

We are also sensitive to the privacy concerns of our employees, as well as our need to effectively deploy and support our work force on a worldwide basis. The ability to transfer human resource data across borders is extremely critical for multinational companies such as GM. We strive to balance very significant and legal and so-

cietal expectations for privacy with the objective of enhancing our customers' ownership experience. With a better understanding of our customers, we can make their shopping, buying, and owning experience more enjoyable, and make the entire process more efficient and cost-effective for GM.

Because the development lead time for vehicles can be up to 3 years long, it is important for us to understand our customers' preferences and the market trends. For example, data on customer purchasing and usage patterns can help us target products more effectively to meet consumer needs, and also to tailor messages and promotions to the interests of current and prospective customers.

We have built a data base about GM vehicle owners to facilitate after-market sales, repairs, next vehicle purchase, and to cross-market the broad range of GM products and services. Customer information is also critical to our U.S. vehicle warranty data base, which is used in the event of a safety or customer satisfaction recall. In addition, customer information may be shared with other parts of the company, so we can enhance the shopping, buying, and owning experiences of our customers with related information and services.

The emergence of new technologies has facilitated more one-to-one communications with our customers. Consequently, we are moving toward a process whereby the consumer will control the type of information they receive, and the manner in which they receive it. The benefits to the customer of this data-rich analysis and cross-marketing focus are increased satisfaction with products and services that are better suited to their needs, and marketing efforts that provide meaningful benefit at the appropriate time and through the communication channel of the consumer's choice.

Attention to the issue of data privacy has been elevated to the highest levels of management at GM. Last fall, a corporate officer assumed responsibility for developing a global data privacy strategy, and my position, which focuses on coordinating our global business units' implementation of GM's privacy strategy, was also created.

We are implementing the strategy on a scheduled basis throughout GM's global marketplace, through the adoption of privacy statements by individual GM business units. The privacy statements will vary by business unit, and the applicable laws, customs, and culture of particular countries. GM already has in place a global information security policy that provides guidelines for appropriate use and handling of GM data.

Again, we appreciate the opportunity to be here today to discuss GM's approach to data privacy, and our ongoing commitment to honoring our customers' privacy preferences. We commend this committee for taking a thoughtful approach to this complex issue, and hope that you will continue to seek industry's input to ensure the approach adopted does not result in legislation that could be burdensome, impractical, and could produce unintended consequences, such as higher consumer costs, prevention of legitimate information collection, and the creation of obstacles to the free flow of information.

Thank you very much.

[The prepared statement of Jacqueline L. Hourigan follows:]

PREPARED STATEMENT OF JACQUELINE L. HOURIGAN, DIRECTOR OF DATA POLICIES, GENERAL MOTORS CORPORATION

Mr. Chairman and members of the subcommittee, my name is Jacqueline Hourigan, and I am the Director of Data Policies for the General Motors Corporation. I welcome the opportunity to appear before the members today to discuss GM's perspectives on the issue of data privacy.

GM appreciates the deliberative and thoughtful approach this committee has taken to the privacy issue. For decades we at GM have worked hard to build strong relationships with the millions of GM customers. These relationships, based on high quality and exciting products and services, are critically important to us. The trust we have established and continue to reinforce through our policies and practices is key to General Motors' success in this extremely competitive automotive and financial services market.

By way of background, General Motors is the world's largest industrial corporation. GM designs, manufacturers, and markets cars, trucks, heavy-duty transmissions, and locomotives worldwide. Other substantial business interests include Hughes Electronics Corporation and General Motors Acceptance Corporation (GMAC). GM cars and trucks are sold in 200 countries and the company has manufacturing or assembly operations in more than 30 countries. GM employs 400,000 people worldwide and partners with over 30,000 suppliers. In 2000, GM sold 8.7 million vehicles worldwide and had revenues of $185 billion.

IMPORTANCE OF THE PRIVACY ISSUE TO GM

The collection, use, and security of personally identifiable data collected on the Internet and in the off-line world are important issues for GM. We seek to align our internal processes and policies with consumer expectations and data privacy laws worldwide. We collect information through a variety of means, such as traditional market research and response techniques, visits to GM web sites, subscriptions to OnStar®, insurance, finance or mortgage products with GMAC, and through in-vehicle technology designed to enhance our customers' safety and security.

GM's privacy concerns also apply to data GM maintains on employees. A key business objective for GM is the effective deployment and support of our workforce. The ability to transfer human resource data across borders is extremely important to companies that have a global footprint, such as ours.

USES OF DATA AND BENEFITS TO CUSTOMERS

GM strives to balance the very significant legal and societal expectations for privacy with the objective of enhancing our customers' ownership experience. With a better understanding of our customers, we can make their shopping, buying, and owning experience more enjoyable and make the entire process more efficient and cost effective for GM.

Because the development lead-time for vehicles ranges from approximately 24 to 36 months, it is important for us to understand customer preferences and market trends. At GM, we apply predictive modeling techniques to the data provided us by our customers to assess trends and forecast our customers' future preferences. The better we understand our customers and where we are gaining or losing sales, the better we can focus our product and marketing priorities.

We also optimize our ongoing marketing efforts by tailoring relevant messages and promotions to our current and prospective customers. Customers generally own their vehicles for many years (almost a decade on average) and we have built a substantial database with information on GM vehicle owners that we use to facilitate after-market sales, repairs, next vehicle purchase, and to cross-market the broad range of GM products and services. It is important to note that customer information is also compiled to populate our U.S. vehicle warranty database so that we can contact customers in the event of a safety or customer satisfaction recall.

Customer information may be shared with other parts of the company. By offering a suite of products and services to our customers their learning, shopping, buying, and owning experience is enhanced. By way of example, GMAC's real estate operation is focused on coordinating realtor, mortgage, closing, moving, homeowner, and relocation services that are critically important to anyone buying a new home. By sharing customer information within the GMAC organization, we can create a seamless service delivery platform that gives time back to the customer and creates real value for them.

The emergence of new technologies has facilitated more one-to-one communications with our customers. Consequently, we are moving toward a process whereby

the consumer controls the type of information they receive and the manner in which they receive it.

The benefits to the customer of this data-rich analysis and cross-marketing focus are increased satisfaction with products and services better suited to their needs and marketing efforts that provide meaningful benefit at the appropriate time and through the communication channel of their choice.

WHAT DATA HANDLING PRACTICES DOES GM EMPLOY

Attention to the issue of data privacy has been elevated to the highest levels of management at General Motors. Last fall, a corporate officer assumed responsibility for developing a global data privacy strategy for the corporation, and my position, which focuses on coordinating our business units' implementation of GM's privacy strategy globally, was also created.

GM is implementing the strategy on a scheduled basis throughout GM's global marketplace through the adoption of privacy statements by individual GM business units. These privacy statements will vary by business unit and the applicable laws, customs, and culture of particular countries. GM already has in place a global information security policy that provides guidelines for appropriate use and handling of data.

CONCLUSION

Again, we appreciate the opportunity to be here today to discuss GM's approach to data privacy and our commitment to respecting our customer's privacy preferences. We commend this committee for taking a thoughtful approach to this complex issue. We hope that you will continue to seek industry's input to ensure the approach adopted does not result in legislation that would be burdensome, impractical and would produce unintended consequences. These unintended consequences could include higher consumer costs, prevention of legitimate information collection, and the creation of obstacles to the free flow of information.

Thank you.

Mr. STEARNS. Thank you.

Mr. Swift?

STATEMENT OF ZEKE SWIFT

Mr. SWIFT. Thank you, Chairman Stearns and members of the subcommittee. I am Zeke Swift, Director of Global Privacy for the Proctor & Gamble Company.

P&G markets 300 brands of consumer products to, as the chairman already mentioned, 5 billion consumers in over 140 countries. These include leading brands like Tide, Pantene, Pringle's, and Iams. We are based in Cincinnati, Ohio, and have on-the-ground operations in over 70 countries.

Privacy is a public policy issue long associated with direct marketing and high-tech industries. So why does P&G, a consumer products manufacturer, care about privacy? Let me summarize our interest in three points.

First, information about consumers is central to a consumer products business. We rely on information to better understand consumer needs and produce products, information, and services to better meet them. As a result, we have an enormous stake in fostering an environment 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 to enable other companies to do the same.

Second, new technologies are enabling us to deliver benefits that were previously impossible. When consumers share information with us, we can now deliver tailored offers, such as samples or coupons, customized products and information, or opportunities to test

new products not yet available in stores. This increases satisfaction among consumers who are interested, and ultimately reduces costs of marketing to consumers who are not. We want to preserve the ability to take full advantage of current and emerging technology to target consumer needs.

Third, handling personal data is a complex issue for a company the size of P&G. We receive consumer data from sources including off-line promotions, online web sites, consumer relations contacts, market research, and clinical studies, just to name a few. We operate in over 70 countries. We have about 200 corporate entities, and relationships with hundreds of vendors and contractors. We have about 375 web sites globally. Administrative processes such as those required by recent European legislation impose an unimagined burden for a company like ours, with little or no substantive benefit to the consumer. We hope that any steps taken in the United States reflect this learning.

Now, let me share two examples of more sophisticated uses of data to meet consumer needs. Both involve interactions with consumers over the Internet.

First, with Reflect.com, a woman provides information about her physical attributes and lifestyle preferences, and then creates personalized skin care, hair care, fragrance, and cosmetic products from some 50,000 possible product combinations. The items are delivered to her door in a personalized package within 3 to 7 business days.

Second, at our Pampers.com web site, parents can sign up for a free monthly newsletter tailored to the age by month of their baby, and delivered to their e-mail inbox. The newsletter offers expert information about raising children, tips from bathing to discipline, coupons, and opportunities to try new products like our Bibster disposable baby bibs—just a word from our sponsor.

In order to deliver these benefits, we collect, obviously, data such as a person's name and address. To increase the tailoring of those offers, we may collect demographic, lifestyle, or product usage information. Consumers give us most of the information we use. In some cases, we get additional information from data compilers such as Acxiom, Equifax, and Experian. And I've given them all equal time because they will be following us in the next panel.

We do not sell personal information. We do share information with vendors acting on our behalf to process data or fulfill a promotion. We do not share data with companies beyond our vendors without the individual's consent.

We are committed to keeping data secure, and take precautions against loss, misuse, or alteration of the data. These measures include physical security, controlled access to data, and encryption for data transmission. We require our vendors and partners to provide privacy practices equivalent to our own, and we forbid them from any additional use of our data.

In conclusion, we believe that understanding consumer needs, delivering consumer benefits, and generating consumer trust, are three pillars that should be at the center of any policy discussion on privacy. If I may paraphrase Representative DeGette from an earlier hearing, there are two secrets about privacy: taking care of

personal information is good for business; and sharing personal information is good for consumers.

Thank you very much.

[The prepared statement of Zeke Swift follows:]

PREPARED STATEMENT OF ZEKE SWIFT, DIRECTOR, GLOBAL PRIVACY, THE PROCTER & GAMBLE COMPANY

INTRODUCTION

Thank you, Chairman Stearns and members of the Subcommittee, for the opportunity to testify on this important issue. My name is Zeke Swift and I am Director, Global Privacy for The Procter & Gamble Company.

As background, Procter & Gamble markets 300 brands of consumer products to nearly five billion consumers in over 140 countries. These brands include Tide, Swiffer, Crest, Pantene Pro-V, Pringles, Pampers, Olay, Iams and Vicks. We are based in Cincinnati, Ohio and have on-the-ground operations in over 70 countries.

KEY MESSAGES

Privacy is a public policy issue long associated with the high tech and direct marketing industries. So why does P&G, a consumer products manufacturer, care about the privacy issue? Let me summarize our interest in three key points.

1. First, *information about consumers is central to our business.* We rely on information to better understand consumer needs, and produce superior products, information and services to meet them. As a result, we have 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.

2. Second, *new technologies are enabling us to deliver a level of benefit on the basis of personal information that was previously impossible.* When consumers share information with us, we now can deliver tailored offers such as samples or coupons, opportunities to test new products, or customized products and information. We want to preserve the ability to take full advantage of current and emerging technology to meet consumer needs.

3. Third, *privacy—or more broadly the way we handle personal data—is a complex issue for a company the size of P&G.* We receive consumer data from many sources including offline promotions, online websites, Consumer Relations contacts, market research and clinical studies. As mentioned, we operate in over 70 countries. We have about 200 corporate entities and relationships with hundreds of vendors and contractors. Administrative processes, such as those imposed by recent European legislation, impose unimaginable burdens for companies like ours with little or no substantive benefit to consumers. We hope that any steps taken in the United States would reflect this learning.

P&G PRIVACY PRACTICES

Now, let me share a couple of points about our overall approach to privacy.

First, we're guided by two fundamental principles:

(a) We strive to treat information provided by individuals as their own, which has been entrusted to us; and

(b) We strive for transparency with consumers about how their information is used. We inform people about how we handle information they provide us. We give them choices about further communication with P&G or further uses of their data. We offer them reasonable access to data they've provided to review it, correct it or ask us not to use it.

Second, we have a long history of responsible treatment of personal information. Our employee privacy policy, for example, dates back more than 20 years. And, we posted our first on-line privacy statement in 1997.

Third, for consistency's sake we've chosen to take a global approach to privacy. We have a single global privacy policy. We have a global structure for developing and implementing our information practices worldwide. We are building a global IT system to implement and monitor our policy globally.

CONSUMER BENEFITS

Now let me provide some examples of the way we're using consumer information today. At the most elemental level, when consumers share their information with

us, we can give them information, services and products tailored to their needs or interests. These may include new product announcements, free sample offers, participation in contests and sweepstakes, and opportunities to test new products not yet available in stores.

But at a more sophisticated level we use interactions with consumers over the Internet to deliver personalized or customized products and services. For example:

1. With *Reflect.com,* a woman provides information about her individual attributes and lifestyle and creates personalized skin care, hair care, fragrances and cosmetics. The items are delivered to her door in a personalized package within 3 to 7 business days. The beauty products are produced from some 50,000 possible product combinations based on P&G formulas.

2. Our *Pampers.com* website strives to be the best resource on the web for parents and parents-to-be. It offers parents an opportunity to sign up for a free monthly newsletter from the Pampers Parenting Institute, tailored to the age of their baby and delivered to their e-mail inbox. The newsletter is full of information about child rearing written by experts, offers tips from bathing to discipline, coupons, and opportunities to sample new products like our disposable Bibster baby bibs.

HOW WE COLLECT AND USE PERSONAL INFORMATION

In order to deliver offers such as these, we collect data such as a person's name, address, email address or phone number so that we may contact them or send them items they have requested. To increase the likelihood that our offers will be of interest, we collect demographic information such as age or gender, lifestyle information such as household status or personal interests, and other relevant information such as product usage and preferences.

Consumers volunteer most of the information we store in our databases. In some situations we use additional demographic information purchased from data aggregators such as Acxiom, Equifax or Experian. The data provided by aggregators is from publicly available sources such as telephone directories and public records, or from information reported by consumers themselves through vehicles such as warranty cards.

We seek to build our relationships with consumers on the basis of transparency and trust. We offer individuals who have provided us with information choices about further communications. We ask whether or not a consumer would like to be contacted about additional offers or services. We seek wherever we can to provide consumers with a convenient means to tell us, yes or no, whether we may use the information they provided to re-contact them.

We do not sell personal information. We obviously do share data with vendors acting on our behalf to fulfill a promotion. We do not share data with companies beyond our vendors without the individual's consent.

We are committed to keeping data secure and take precautions against loss, misuse or alteration. These measures include physical security, controlled access to data and encryption for data transmission. We require vendors, partners and contractors to provide equivalent privacy measures and forbid them to use data for any additional purpose.

SUMMARY

In conclusion, we believe that understanding consumer needs, delivering consumer benefits and generating consumer trust are the issues at the heart of any policy discussion on privacy. If I may paraphrase Representative DeGette from an earlier subcommittee hearing, "There are two secrets about privacy: privacy—the stewardship of personal information—is *good* for business, and information sharing is *good* for consumers."

Thank you.

Mr. STEARNS. Thank you.

Mr. Misener, your opening statement?

STATEMENT OF PAUL MISENER

Mr. MISENER. Thank you, Chairman Stearns and members of the subcommittee. My name is Paul Misener. I am the Vice President for Global Public Policy at Amazon.com. Thank you very much for inviting me here to testify today.

Mr. Chairman, Amazon.com is pro-privacy. The privacy of personal information is important to our customers, and thus it is im-

portant to us. Indeed, as Amazon.com strives to be the Earth's most customer-centric company, we must provide our customers the very best shopping experience, which is a combination of convenience, personalization, privacy, selection, savings, and other features. At Amazon.com, we manifest our commitment to privacy by providing our customers notice, choice, access, and security.

Before I describe these four facets of privacy protection at Amazon.com, please allow me to explain how we use customer information. In general, Amazon.com uses personally identifiable customer information to personalize the shopping experience at our store. Rather than present an identical storefront to all visitors, our longstanding objective is to provide a unique store to every one of our customers, now totaling well over 35 million people. In this way, our customers may readily find the items they seek, and discover other items of interest.

Amazon.com now inserts, among the familiar tabs across the top of our web pages, a special tab with our customer's name on it. When I visited Amazon's site on Monday, for example, the tabs included books, electronics, DVDs, and "Paul's store." By clicking on the "Paul's store" tab, Amazon.com introduced me to six smaller stores, including one named "Your kitchen and housewares store," which featured a Calphalon professional nonstick 5-quart saucepan, which I promptly bought, and it was delivered yesterday.

Now, it was no coincidence, of course, that Amazon.com recommended this saucepan to me, and that I liked it. Using so-called collaborative filtering techniques, which compare my past purchases to anonymous statistics on thousands of other Amazon.com purchases, Amazon.com computers automatically, and correctly, predicted that I would want this saucepan. Similar personalization is provided in the traditional Amazon.com recommendations on the home page, and purchase follow-up recommendations in the "New for You" feature, and in some varieties of e-mail communications.

Obviously, Amazon.com's personalization features directly benefit our customers. And just as obviously, these features require the collection and use of personally identifiable customer information. The question then is how do we protect the privacy of this information?

As I indicated earlier, Amazon.com manifests its privacy commitment by providing notice, choice, access, and security. Amazon.com was one of the very first online retailers to provide a clear and conspicuous privacy notice. We also provide our customers meaningful privacy choices. In some instances we provide opt-out choice, and in other instances we provide opt-in choice.

We are an industry leader in providing our customers access to the information we have about them. They may easily view and correct, as appropriate, their contact information, payment methods, purchase history, and even the clickstream record of products they view while browsing Amazon.com's online stores. And finally, Mr. Chairman, Amazon.com vigilantly protects the security of our customers' information.

It is very important to note here that, other than an obligation to live up to pledges made in our privacy notice, there is no legal requirement for Amazon.com to provide our customers the privacy protections that we do. So why do we provide notice, choice, access,

and security? The reason is simple: privacy is important to our customers, and thus it is important to Amazon.com. We simply are responding to market forces. Indeed, if we didn't make our customers comfortable shopping online, they will shop at established brick-and-mortar retailers, who are our biggest competition.

These market realities lead us to conclude that there is no inherent need for privacy legislation. That said, we have been asked whether Amazon.com could support a privacy bill. Perhaps we could, but only under certain circumstances.

At the Federal level, Amazon.com could support a bill that would require notice and meaningful choice, but only if it would pre-empt inconsistent State laws, bar private rights of action, and address both online and off-line activities. Please allow me to explain each of these points.

First, any Federal privacy legislation applied to online activities must pre-empt inconsistent State laws, for it would be virtually impossible for a nationwide web site to comply with conflicting rules from multiple jurisdictions.

Second, Amazon.com could support a privacy bill only if it would bar private rights of action. The threat of aggressive private litigation would companies to balkanize their privacy notices for the sake of legal defensibility, at the expense of simplicity and clarity.

Third and finally, Amazon.com believes that privacy legislation must apply equally to online and off-line activities. It makes little sense to treat information collected online differently from the same, and often far more sensitive, information collected through other media, such as mail-in warranty registration cards, point-of-sale purchase tracking, and magazine subscriptions.

On one hand, such parity is necessary in fairness to online companies. But more importantly, it would be misleading to American consumers to enact a law that applies only to online entities, because for the foreseeable future the putative protections of such a law would apply only to a very tiny fraction of consumer transactions. Last year, online sales accounted for less than 1 percent of all retail business. Obviously, any law that addresses only online transactions could not benefit consumers much at all compared to one that equally addresses online and off-line activities.

Moreover, to the extent it provides any real consumer benefits, a law that addresses only online activities would have the perverse effect of failing to provide any benefits to those on the less fortunate side of the digital divide. Indeed, consumers who, because of economic situation, education, or other factors, are not online, would receive no benefits of a new online-only law.

In sum, Mr. Chairman, Amazon.com is pro-privacy in response to consumer demand and competition. We believe market forces are working, and thus believe there is no inherent need for legislation. Nonetheless, Amazon.com could support limited Federal legislation, but only if it pre-empts State laws, only if it bars private rights of action, and only if it applies to off-line as well as online activities.

Thank you again for inviting me to testify. I look forward to your questions.

[The prepared statement of Paul Misener follows:]

PREPARED STATEMENT OF PAUL MISENER, VICE PRESIDENT, GLOBAL PUBLIC POLICY, AMAZON.COM

Chairman Stearns, Mr. Towns, and members of the Subcommittee, my name is Paul Misener. I am Amazon.com's Vice President for Global Public Policy. Thank you for inviting me to testify today.

A pioneer in electronic commerce, Amazon.com opened its virtual doors in July 1995 and today offers books, electronics, toys, CDs, videos, DVDs, kitchenware, tools, and much more. With well over 30 million customers in more than 160 countries, Amazon.com is the Internet's number one retailer.

Mr. Chairman, Amazon.com is pro-privacy. The privacy of personal information is important to our customers and, thus, is important to us. Indeed, as Amazon.com strives to be Earth's most customer-centric company, we must provide our customers the very best shopping experience, which is a combination of convenience, personalization, privacy, selection, savings, and other features.

At Amazon.com, we manifest our commitment to privacy by providing our customers notice, choice, access, and security. Before I describe these four facets of privacy protection at Amazon.com, please allow me to explain how we use customer information.

In general, Amazon.com uses personally identifiable customer information to personalize the shopping experience at our store. Rather than present an identical storefront to all visitors, our longstanding objective is to provide a unique store to every one of our customers, now totaling well over 35 million people. In this way, our customers may readily find items they seek, and discover other items of interest. If, for example, you buy a Stephen King novel from us, we likely will recommend other thrillers the next time you visit the site.

Amazon.com now inserts, among the familiar "tabs" atop our Web pages, a special tab with the customer's name on it. When I visited Amazon.com's site yesterday, for example, the tabs included Books, Electronics, DVDs, and "Paul's Store." By clicking on the "Paul's Store" tab, Amazon.com introduced me to six smaller stores, including one named, "Your Kitchen and Housewares Store," which featured a Calphalon professional nonstick 5-quart saucepan (which I promptly bought).

It was no coincidence, of course, that Amazon.com recommended this saucepan to me, and that I liked it: using so-called "collaborative filtering" techniques, which compare my past purchases to anonymous statistics on thousands of other Amazon.com purchases, Amazon.com computers automatically—and correctly—predicted that I would want the saucepan.

Similar personalization is provided in the traditional Amazon.com recommendations on the home page, in purchase follow-up recommendations, in the "New for You" feature, and in some varieties of email communications. Customers can improve the quality of these recommendations in several ways, including by removing individual Amazon.com purchases from consideration, and by rating the products they buy at Amazon.com or elsewhere. For example, I bought my niece a few CDs from the singer Britney Spears but, because I did not want similar music recommended to me, I removed these CDs from the list of items Amazon.com uses to produce my recommendations. In addition, on Amazon.com's site, I can rate a CD that I might have purchased at Wal-Mart to improve the quality of my music recommendations.

Obviously, Amazon.com's personalization features directly benefit our customers. And, just as obviously, these features require the collection and use of personally identifiable customer information. The question, then, is how do we protect the privacy of this information?

As I indicated earlier, Amazon.com manifests its privacy commitment by providing notice, choice, access, and security.

Notice. Amazon.com was one of the first online retailers to post a clear and conspicuous privacy *notice.* And last summer, we proudly unveiled our updated and enhanced privacy policy by taking the unusual step of sending email notices to all of our customers, then totaling over 20 million people.

Choice. We also provide our customers meaningful privacy *choices.* In some instances, we provide opt-out choice, and in other instances, we provide opt-in choice. For example, Amazon.com will share a customer's information with a wireless service provider only after that customer makes an opt-in choice. We simply are not in the business of selling customer information and, thus, beyond the very narrow circumstances enumerated in our privacy notice, there is no information disclosure without consent.

Access. We are an industry leader in providing our customers access to the information we have about them. They may easily view and correct as appropriate their

contact information, payment methods, purchase history, and even the "clickstream" record of products they view while browsing Amazon.com's online stores.

Security. Finally, Amazon.com vigilantly protects the *security* of our customers' information. Not only have we spent tens of millions of dollars on security infrastructure, we continually work with law enforcement agencies and industry to share security techniques and develop best practices.

It is very important to note that, other than an obligation to live up to pledges made in our privacy notice, there is no legal requirement for Amazon.com to provide our customers the privacy protections that we do.

So why do we provide notice, choice, access, and security? The reason is simple: privacy is important to our customers, and thus it is important to Amazon.com. We simply are responding to market forces.

Indeed, if we don't make our customers comfortable shopping online, they will shop at established brick and mortar retailers, who are our biggest competition. Moreover, online—where it is virtually effortless for consumers to choose among thousands of competitors—the market provides all the discipline necessary. Our customers will shop at other online stores if we fail to provide the privacy protections they demand.

These market realities lead us to conclude that there is no inherent need for privacy legislation. That said, we have been asked whether Amazon.com could support a privacy bill. Perhaps we could, but only under certain circumstances.

Under no circumstances would we support state or local laws governing online privacy. Not only would such laws be constitutionally suspect, a nationwide website like Amazon.com would find it difficult if not impossible to comply with fifty or more sets of conflicting rules.

At the federal level, Amazon.com could support a bill that would require notice and meaningful choice, but only if it would preempt inconsistent state laws, bar private rights of action, and address both online and offline activities. Please allow me to briefly explain each of these points.

Preempt State Law. First, any federal privacy legislation applied to online activities must preempt inconsistent state laws, for it would be virtually impossible for a nationwide website to comply with conflicting rules from multiple jurisdictions. Even though such laws most likely would fail a constitutional challenge, the expense and uncertainty of litigation should be avoided with a Congressionally adopted ceiling.

Bar Private Rights of Action. Second, Amazon.com could support a privacy bill only if it would bar private rights of action. The threat of aggressive private litigation would cause companies to balkanize their privacy notices for the sake of legal defensibility, at the expense of simplicity and clarity. Ten-page privacy statements and fine-print legalese would become the norm. A regulatory body such as the Federal Trade Commission, on the other hand, could balance the competing interests of legal precision and simplicity. A class action plaintiffs' lawyer would have no such motivation.

In addition, the aforementioned uniformity necessary to run nationwide websites would be destroyed by a host of trial lawyers suing companies all across the country. A single authority, such as the FTC, could provide the nationwide approach that private litigation cannot.

Parity with Offline Activities. Third, and finally, Amazon.com believes that privacy legislation must apply equally to online and offline activities, including the activities of our offline retail competitors. It makes little sense to treat information collected online differently from the same—and often far more sensitive—information collected through other media, such as offline credit card transactions, mail-in warranty registration cards, point-of-sale purchase tracking, and magazine subscriptions.

On one hand, such parity is necessary in fairness to online companies. It simply would not be equitable to saddle online retailers with requirements that our brick-and-mortar or mail order competitors do not face.

But more importantly, it would be misleading to American consumers to enact a law that applies only to online entities because, for the foreseeable future, the putative protections of such a law would apply only to a tiny fraction of consumer transactions. Last year, online sales accounted for less than one percent of all retail business. Obviously, any law that addresses only online transactions could not benefit consumers much at all compared to one that equally addresses online and offline activities such as using a grocery store loyalty card or subscribing to a magazine.

Moreover, to the extent it provides real consumer benefits, a law that addresses only online activities would have the perverse effect of failing to provide any benefits to those on the less fortunate side of the digital divide. Indeed, consumers who,

because of economic situation, education, or other factors, are not online would receive no benefits from a new, online-only law.

In sum, Mr. Chairman, Amazon.com is pro-privacy in response to consumer demand and competition. We believe market forces are working and, thus, believe there is no inherent need for legislation. We firmly oppose the adoption of any nonfederal privacy law that addresses online activities. Nonetheless, Amazon.com could support limited federal legislation, but only if it preempts state laws, only if it bars private rights of action, and only if it applies to offline as well as online activities.

Thank you again for inviting me to testify, I look forward to your questions.

Mr. STEARNS. Thank you.

Mr. Johnson, your opening statement?

STATEMENT OF DAVID A. JOHNSON

Mr. JOHNSON. Mr. Chairman and members of the subcommittee——

Mr. STEARNS. You might just pull the microphone a little closer and just maybe straighten it—yes.

Mr. JOHNSON. Okay. Mr. Chairman and members of the subcommittee, I am pleased to appear before you today on behalf of the National Retail Federation, and thank you for the invitation to speak on this important issue. My name is David Johnson, and I am Vice President of Direct Marketing for Land's End in Dodgeville, Wisconsin.

Although we are now an international merchant, many of the things that today sets Land's End apart are those same values on which our founder, Gary Comer, built the business he founded in 1963. Indeed, one of the principles that continues to guide our business states: "We believe that what is best for the customer is best for all of us."

When people are asked to define good customer service, they commonly say that it involves dealing with consumers honestly and fairly, a view that no one can seriously dispute. Many others also view a component of good customer service as treating everyone equally. Let me suggest, however, that equal treatment is not good customer service. Rather, great customer service recognizes the very unique wants and needs of each individual consumer, and strives to meet those needs. Great customer service uses all available information to assess each individual's particular tastes, and then delivers goods and services that meets those desires. In short, rather than treating all customers equally, great customer service is built on the premise of treating different customers differently.

In testimony before Congress in July 1999, Federal Reserve Board Governor Edward Gramlich stated: "Information about individuals' needs and preferences is the cornerstone of any system that allocates goods and services within an economy." The more such information is available, he continued, "the more accurately and efficiently will the economy meet those needs and preferences." What Governor Gramlich was talking about on a macro level, Land's End is striving to do on a micro level.

The information required to provide these tailored interactions with our customers does come from a wide variety of sources. We look to our customer purchase history and other acquired information in order to more reliably assess our customers' needs and wants. By assessing information on purchases that consumers actually make, and services that they actually use, consumers are of-

fered products and services that respond to their demonstrated needs and desires. This greatly reduces the cost of developing those products and services, and the risk that they will be out of line with consumer demand, thereby reducing the price that consumers pay for them, and mitigating the inconvenience and delay associated with stopping consumers to ask about likely preferences.

Admittedly, we often hear complaints about customers receiving mailings that they don't want. But Land's End—and I strongly suspect every other direct merchant—has no interest in sending catalogues or other information to customers that have no desire to receive it. Frankly, that is a waste of our time and money, and a disservice to the customer. Thus, we use all information available to us to assess the likelihood that any catalogue sent will be welcome in the customer's home. To the extent that cataloguers send mailings to people who are not interested in the offering, I suggest that the problem is not one of too much information sharing, but rather too little reliable information, forcing businesses to employ mass marketing techniques instead of more targeted efforts to a more appropriate and appreciative audience.

Moreover, the ability to collect and assess individual purchasing activity gives Land's End the ability to provide services to customers that we might not otherwise. As an example, Land's End sells its products with a guarantee that is second to none. Under our "Guaranteed. Period." policy, any customer can return any product, at any time, for any reason. A guarantee this sweeping is by its nature subject to abuse, and by offering it Land's End has placed unprecedented faith in its customers that they will not exploit the policy.

But we comfort in offering our "Guaranteed. Period." policy, because it is enhanced by the ability of individualized purchasing and return data that allow us to track and check abuses. In short, this information ensures that the few that might exploit the guarantee don't ruin it for the overwhelming majority of our customers that are fair and reasonable.

And consistent with the trust and loyalty that our customers have shown us, Land's End is also quite responsible with the information we share with others. Indeed, the only data we currently provide to others are one-time use list exchanges, which include only customers' names and addresses, and then only with high-quality companies that share our commitment to product quality, customer service and value, and could, therefore, offer products and services attractive to Land's End customers. And regardless of the medium by which we interact with the customer—the Internet, phones, or mail—customers may at any time request that their information not be shared with others, or that they be removed from our files altogether. And that is a request that will be honored. Guaranteed. Period.

So in answer to the question posed by this hearing—"Is the Customer's Privacy Protected?"—the good news is that currently available information is used responsibly, consistent with the expectations of consumers, and in furtherance of everyone's interest, the consumer's, as well as the companies that serve them.

Again, thank you for this opportunity to speak this morning, and I welcome your comments and questions.

[The prepared statement of David A. Johnson follows:]

PREPARED STATEMENT OF DAVID A. JOHNSON, VICE PRESIDENT, DIRECT MARKETING, LANDS' END, INC. ON BEHALF OF THE NATIONAL RETAIL FEDERATION

Mr. Chairman and Members of the Subcommittee: I am very pleased to appear before you today on behalf of the National Retail Federation, and thank you for the invitation to speak on this subject. My name is David Johnson, and I am Vice President of Direct Marketing for Lands' End, Inc., in Dodgeville, Wisconsin. Lands' End employs approximately 7,600 people in the U.S. and abroad. We are a global direct merchant of classically-inspired clothing for men, women and children, soft luggage and products for the home, sold through regular mailings of our catalogs, our Web site—landsend.com—and a number of retail outlets. Last year, Lands' End's revenues exceeded $ 1.4 billion, and we mailed packages to approximately 6.7 million customers.

The National Retail Federation (NRF) is the world's largest retail trade association with membership that comprises all retail formats and channels of distribution including department, specialty, discount, catalog, Internet and independent stores. NRF members represent an industry that encompasses more than 1.4 million U.S. retail establishments, employs more than 20 million people—about 1 in 5 American workers—and registered 2000 sales of $3.1 trillion. NRF's international members operate stores in more than 50 nations. In its role as the retail industry's umbrella group, NRF also represents 32 national and 50 state associations in the U.S. as well as 36 international associations representing retailers abroad.

Although we are now an international merchant, many of the things that today set Lands' End apart are those same values on which our founder, Gary Comer, built the business he founded in 1963. Indeed, one of the principles that continues to guide our business states: "We believe that what is best for our customer is best for all of us. Everyone here understands that concept. Our sales and service people are trained to know our products, and to be friendly and helpful."

Through this dedication to the customer, Lands' End has been able to separate itself from the pack in customer service. Indeed, in the book *Customer Service*,[1] author Fred Wiersema lauds Lands' End (along with five other companies) for its ability to service the customer above and beyond the call of duty.

When people are asked to define good customer service, they commonly say that it involves dealing with consumers honestly and fairly, a view that no one can seriously dispute. Many others also view a component of good customer service as treating everyone *equally*. Let me suggest, however, that equal treatment is not good customer service. Rather, great customer service recognizes the very unique wants of each individual consumer and strives to meet those needs. Thus, great customer service does not view every customer as a nameless, faceless person without individual preferences—someone that in the absence of any other information needs to be treated just like the next person. Instead, great customer service uses all available information to assess each individual's particular tastes, and then deliver goods and services that meet those desires. In short, rather than treating all customers equally, great customer service is built on the premise of *treating different customers differently*.

Access to information is critical to our ability to deliver this level of service. Information is used to identify and satisfy customer needs. Lands' End does not automatically know which products and services consumers want. Information beyond a person's name and address allows us to tailor our interaction with the customer to make it more effective and more satisfying for the consumer. As Mr. Wiersema states in his book Customer Service, two of the most key components underlying the ability to provide exceptional customer service are (1) the employment of up-to-date information technology, and (2) the personal, one-to-one relationship built with every customer.

> "Although they conduct their business in completely different areas of industry, these organizations actually have many things in common with regard to how they function:
>
> * * *
>
> "They employ the latest information technology at each level of their business. This shouldn't be surprising: Information technology lends itself to strong customer service, and early on, these companies all recognized the advantages, the instant gratification, that the Internet and other technological advances could

[1] Customer Service by Fred Wiersema (Harper-Collins Publishers, Inc. 1998).

offer them. Rather than trying to dazzle the customer with the latest bells and whistles, they use technology to make their products and services easier to acquire and operate—as well as more efficient.

* * *

"...[T]hey use that technology to gain a profound understanding of what these customers want and need. The notion of building profiles on every customer they interact with is important to them. If Customer A likes something different from Customer B, these companies want to know that ahead of time...

* * *

"These companies build personal relationships with their customers. They are not mass-production factories when it comes to connecting with their constituents. Each customer who deals with these organizations is given premium treatment and made to feel he or she is valued as an individual, able to call a service representative time and again...

This degree of one-to-one attention requires a commitment to training, to coaching, and to teaching associates the best listening strategies and most efficient methods for giving and receiving input. It takes computer technology, as well as dedicated personnel willing to record each customer interaction onto databases so that it can be activated later and used as a learning tool for fellow workers."[2]

In testimony before Congress in July 1999, Federal Reserve Board Governor Edward Gramlich stated: "Information about individuals' needs and preferences is the cornerstone of any system that allocates goods and services within an economy." The more such information is available, he continued, "the more accurately and efficiently will the economy meet those needs and preferences." What Governor Gramlich was talking about on a macro level, I can guarantee Lands' End is striving to do on a micro level.While many of our customers love the technology and the wealth of information that is available over the Internet, many other customers want the direct interaction that they can get over the phone from one of our highly trained customer sales representatives. We are agnostic as to how we interact with the customer—whether it be through the Internet, the phone, mail or one of our outlet stores—but we do need to know *their preferences* in order to build the infrastructure necessary to effectively communicate with them via their preferred medium. We also need to know our customers' preferences with respect to the products and services available—either now or in the future—to our customers. While some would prefer to learn about the entire array of Lands' End product offerings, others' interests are more limited and they would prefer to only receive catalogs from a certain selection of our assortment of apparel and home goods. This type of information educates us not only on what we should be communicating to our customers *today*, but also provides Lands' End with information on every detail—including assortment, color, fit, level of quality, and price—that we should provide in future products and services.

The information required to provide these tailored interactions with our customers comes from a wide variety of sources. One obvious source is the customer himself or herself in the form of preference surveys. It is possible to extensively survey customers to determine their individual preferences, but such data is not only expensive to acquire, its acquisition runs contrary to the customer service commitment of an organization such as Lands' End. Frankly, it is a bother for a customer to complete questionnaires telling businesses what they expect in products and services. Because of these limitations, such direct information is oftentimes unavailable and somewhat unreliable. For that reason, we look to customer purchase history and other acquired information in order to more reliably assess our customers' needs and wants. By assessing information on purchases that consumers *actually* make and services they *actually* use, consumers are offered products and services that respond to their demonstrated needs and desires. This greatly reduces the cost of developing those products and services and the risk that they will be out of line with consumer demand—thereby reducing the price that consumers pay for them—and mitigating the inconvenience and delay associated with stopping consumers to ask about likely preferences.

Admittedly, we often hear complaints about customers receiving mailings that they don't want. But Lands' End—and I strongly suspect every other direct merchant—has no interest in sending catalogs or other information to customers who

[2] *Customer Service* at xiv-xviii.

have no desire to receive it. Frankly, that is a waste of our time and money, and frustrating to the consumer as well. Thus, we use all information available to us to assess the likelihood that any catalog we send out will be welcome in the customer's home. To the extent that cataloguers send mailings to people who are not interested in the offering, I suggest that the problem is not one of too much information sharing but rather too little reliable information, forcing businesses to employ mass marketing techniques instead of more targeted efforts to a more appropriate and appreciative audience.

Moreover, the ability to collect and assess individual purchasing activity gives Lands' End the ability and comfort to provide enhanced services to customers that we might not otherwise. As an example, Lands' End sells its products with a guarantee that is second to none. Under our "Guaranteed. Period.®" policy, any customer can return any product at any time for any reason. A guarantee this sweeping is, by its nature, subject to abuse, and by offering it Lands' End has placed unprecedented faith in its customers that they will not exploit the return policy. But Lands' End's comfort in offering our "Guaranteed. Period.®" policy is enhanced by the availability of individualized purchasing and return data that allows us to track and check abuses. In short, this information assures that the few that might exploit the guarantee don't ruin it for the overwhelming majority of our customers that are fair and reasonable in their returns.

Likewise, the availability of certain products and services by their nature—and particularly so of many of the services available over the Internet—all but require that some information be shared among companies. As examples, Lands' End offers online models which a customer can use to virtually "try on" clothes, and a "personal shopper" that, applying conjoint analysis techniques, offers purchasing recommendations to online shoppers much as a sales clerk would do in a retail store. For these types of services to become accepted and useful to the consumer, they must also become standardized throughout industry with the individualized models and preferences portable from site to site. This type of information sharing will ultimately enhance the breadth of products and services available to the consumer.

And consistent with the trust and loyalty that our customers have shown us, Lands' End is also quite responsible the information we share with others. Indeed, the only data we currently provide to others are one-time-use list exchanges, which include only customers' names and addresses, and then only with high quality companies that share Lands' End's commitment to product quality, customer service and value and could, therefore, offer products and services attractive to Lands' End customers. And regardless the medium by which we interact with our customer—the Internet, phones or mail—customers may at any time request that their information not be shared with others, or that they be removed from our files altogether, and that request will be honored.

So in answer to the question posed by this hearing—"Is the Customer's Privacy Protected?"—the good news is that currently available information is principally shared responsibly, consistent with the expectations of consumers and in furtherance of everyone's interests—the consumer's as well as the companies that serve them.

Again, thank you for this opportunity to speak before this Subcommittee, and I welcome your questions and comments.

Mr. STEARNS. I thank the panel. Let me start by asking some of the basic questions I think all consumers are concerned about. And this sort of touches into what Mr. Hourigan had talked about—that they build a substantial data base with information on GM vehicle owners, and that GM uses this to facilitate after-market sales, repairs, next vehicle purchase, and to "cross-market the broad range of GM products and services." Is this a singular data base?

Ms. HOURIGAN. It is not a singular data base. We have separate data bases. The data base that I mentioned is primarily used for market segmentation, and in our product development phase.

Mr. STEARNS. Give me, for example, examples of the type of information that is contained in this data base. Other than the ones I mentioned, is it pretty much just the name of the owner, the purchase? Are there preferences and things that are in this data base?

Ms. HOURIGAN. It actually is, if I can mention one thing, our divisions have operated on a tremendously autonomous basis for

many years. And we just recently have elected to streamline many of our processes and practices. Data handling is one such practice.

And so what we have attempted to do is, again, move toward a process by which all divisions will operate under the same policies and practices. The information that is contained in that data base is vehicle name and type of vehicle. We will augment that with information we obtain from the aggregators, but again, it is only for the purpose of market segmentation.

Mr. STEARNS. How do you protect that information? For example, within the company, and also protect it when you deal with subcontractors, or other organizations that you deal with?

Ms. HOURIGAN. Well, we obviously use the highest standards of security to protect the information. We also use managerial security techniques, along with physical security measures.

In terms of working with our suppliers, we obviously only deal with credible suppliers to process the transactions on behalf of our customers. We also have contractually limited how our suppliers can use that information for any subsequent purposes.

Mr. STEARNS. Mr. Misener has talked about not having legislation, but if we have legislation, he would say it should be three items: pre-emptive rights, of course, so that if States start to develop it, that there would be Federal legislation to pre-empt the States, so you wouldn't have to comply with 50 States; what would apply to online would also apply to off-line; and then he talked about private rights of action.

And just for the benefit, the private rights of action, we, of course, on this committee would not all agree with this, but basically this would prevent class actions suits as I understand it against you individuals, based upon something that perhaps you compromised privacy, and then this would turn out to be, among thousands of people who would come together with a class-action suit.

Now, he mentioned those three that he would like to see, if there is Federal legislation. Are there any other ones? And I will just go from my left to my right and ask each of you if there are any besides those three? And if you disagree with Mr. Misener, that you don't think they should be part of this, now is the time to tell us.

Ms. PEARSON. I would agree with those three features being reflected that way in possible legislation. I would just go back to the point of, as your committee has begun a process of deliberation and understanding how information flows in our economy, and how consumers can be affected by that information, is to start with a more fundamental question: where is the issue that needs to be addressed? Once we understand what companies do with information, what government does with information, and then go from there.

I think if there is legislation affecting commercial practices, there ought to be some level of understanding of why commercial practices versus other kinds of uses of information. So there ought to be that.

Mr. STEARNS. I could give you a list of what I think the consumer wants. But I am just asking you now, just, because I don't have a lot of time, just quickly to go through and say, Yes, I think those three are the basic——

Ms. PEARSON. Yes, I think those three features are basic.

Mr. STEARNS. Basic for Federal legislation?

Ms. PEARSON. Yes.

Mr. STEARNS. Is there anything you would add to it?

Ms. PEARSON. I think there ought to be technology neutrality, so that you don't get into specific requirements about this technology or that technology being used, so that you accommodate flexible changes. The world is changing extremely rapidly, and we need to have that ability to innovate. There ought to be, I think, some basic guidelines so that you encourage transparency in information practices without requiring specific content for notices or specific practices. Those are two.

Mr. STEARNS. Okay.

Ms. HOURIGAN. I would just second what Harriet said, technology-neutral, in addition to what Mr. Misener mentioned earlier.

Mr. STEARNS. Okay. Mr. Swift?

Mr. SWIFT. The one addition that we would have is that the legislation would recognize the role of industry self-regulation, and possibly the role of TrustMark programs in the self-regulatory process.

Mr. STEARNS. What does that last part mean?

Mr. SWIFT. A BBBOnLine or Trustee, a program that validates and sets criteria for appropriate practices.

Mr. STEARNS. Best business practices?

Mr. SWIFT. Correct.

Mr. STEARNS. Okay. Mr. Misener?

Mr. MISENER. I thought Mr. Misener's list was pretty good.

Mr. STEARNS. I thought so, yeah.

Mr. Johnson?

Mr. JOHNSON. We believe that any legislation should move incrementally, and allow us to really understand the impact that it ultimately has in helping us to serve our customers.

Mr. STEARNS. Okay, my time has expired, and we are eager to hear other members. But I think, just briefly in the 5 minutes I have had, you have outlined what, if any, Federal legislation should include. And I think that is the purpose, to get from you your heartfelt opinion of what we should do. And we have come up with 1, 2, 3, 4, 5, 6, 7 components of this Federal legislation.

I am very pleased to welcome the ranking member, the gentleman from New York, Mr. Towns.

Mr. TOWNS. Thank you very much, Mr. Chairman. Let me say that I am happy that you are having this hearing. I think it is so important that we listen to people before we move forward on legislation.

I would like to know, I guess, Mr. Misener, what do you deem as an appropriate penalty for those companies who abuse consumer privacy, by breaking their own privacy laws? What would you consider an adequate penalty?

Mr. MISENER. An adequate penalty? Well, certainly it would depend upon a lot of factors going into the abuse. If it is repetitive, if it is willful, intentional, deliberate—all those sorts of things—then I would think that the penalty could be greater. But those are the sorts of issues that, for example, the Federal Trade Commission could take into account.

If a privacy policy is announced by a company, and then not followed by that same company, the Federal Trade Commission, under its powers in Section 5 of the Federal Trade Commission Act, could go after that company and apply a variety of remedies, including injunction and fines.

Mr. TOWNS. Let me ask you, if I buy ten books through your company, are those records available to data collectors? In other words, do you sell the products that I purchase through Amazon.com to data collectors?

Mr. MISENER. Yes, that is an excellent question, Mr. Towns. Absolutely not. Amazon.com is emphatically not in the business of selling customer information. We do not transfer that information to unaffiliated third parties at all. And for the few affiliated third parties, we transfer it only with opt-in consent from our customers.

Mr. TOWNS. On that note, Mr. Chairman, I yield back.

Mr. STEARNS. Okay. I thank the gentleman. We have the distinguished chairman of the full committee, the gentleman from Louisiana, Mr. Tauzin.

Chairman TAUZIN. I thank you, Mr. Chairman. Again, thank you for this series of hearings, because I think they are better preparing this committee, and hopefully the Congress, for whatever privacy decisions we need to make, either generally or, as some of you point out, incrementally.

Let me first say that one of the concerns I have as we explore all the edges of this privacy debate, is that we very carefully remember that we ought to avoid solutions simply looking for problems. It is easy to do in this area. It is easy to begin imagining how data could be misused and how people might do something with data, and then make a great deal of complex Federal laws and solutions designed to fit imagined problems. And what you are doing, Mr. Chairman, is actually focusing on the real world, the reality of how data is exchanged, and how the industry is really working for its own customers' sake and its own business self-interest, in building self-regulatory regimes and regulating itself. And that is an important part of this process, I think, understanding where the real problems are, not the imagined ones.

In that regard, in the very short time we each have, I want to do just one thing with this very important panel. I would like each of you to answer this question in order, and I will be very satisfied with my 5 minutes. It is a very basic question, and it is a question that goes to what is probably the most important decision we first make on privacy. And that is whether to make privacy policy Internet-specific or not.

Now, you all operate your businesses in different ways, online and off-line. Some of you are strictly online. But the question I have is that, recognizing that if we made privacy policy that was Internet-specific—which could, theoretically, prejudice commerce against online activities in favor of off-line activities—recognizing that, is there a good reason to make privacy policy special and different and unique for the Internet world, the online world, as opposed to making it consistent for all activities, whether it is online or off-line?

If each of you will comment on that in a row, I would deeply appreciate it.

Ms. PEARSON. I get to start. From IBM's point of view, it is the same data base or set of data bases, in back of that curtain, that receive the information, no matter where it comes from. So our view has been that if we are going to be deliberative about this, we ought to realize that. And therefore, particularly since the Internet is so new as a mechanism for communicating, that we ought to think about all the media equally—that there shouldn't be a disadvantaging of the Internet over other media. That is a starting point for discussion.

Chairman TAUZIN. Okay. As you go down, I want—if any of you have a good reason to believe that the Internet is so different that it needs special rules, if you don't mind commenting on that. Please?

Ms. HOURIGAN. Sure. I think—we actually had this exact debate in our company, as to whether it was appropriate to apply a different set of standards to the Internet. And we came to the conclusion that it did not.

However, I think to the extent that there may be specific abuses that may occur in the online world that would not exist in the off-line world, then it may be appropriate to treat those particular instances differently. But for General Motors, we still collect a tremendous amount of information off-line, and so to apply different standards would be challenging. And, you know, it is complex enough as it is, I guess. So, thank you.

Chairman TAUZIN. Thank you.

Mr. SMITH. Let me answer by just talking about how we are looking at this within P&G. Our dream is that we would be able to bring together information that we have about a single consumer, regardless of how that information was collected—through consumer relations contact, a web site, whatever. And the reason is that when the consumer calls the next time, or when we make an offer, we would like to reflect everything we know about that consumer. And when we recognized that, we said, we need to apply the same information practices to all the data, because it is going to end up in the same place.

So, you know, we would obviously believe that looking at that information, regardless of its source, regardless of where it is stored, being treated in the same way.

Mr. MISENER. Mr. Tauzin, we strongly believe at Amazon.com that any new legislation ought to apply both to the online and the off-line worlds. There are a couple of reasons. One is the fundamental fairness that you mentioned to online companies who would be potentially burdened by a new regulation that would not apply to our off-line competitors.

But more fundamentally, it is a consumer issue. Consumers spent, in the retail world, 99-plus percent of their dollars in the off-line world. Less than 1 percent of the retail transactions were made online. And so an online-only law is going to do very, very little for consumers more broadly.

Moreover, the consumers that it would help, that it would effect, would be only those on the fortunate side of the digital divide. If you don't have the education or money to be shopping online, that privilege, you would get no benefits from an online-only law.

Mr. JOHNSON. Mr. Tauzin, we believe that there is not a reason to make it Internet-specific per se. Our customers shop with us via the phone, via the Internet. Many of our customers interact with us through numerous different ways.

One position that we do take, however, is that there is a need to be sure that we really understand the implications that it may have on companies like us that are a multi-channel business, and the implications in the long run that it may have for the consumer in ultimately providing the high level of customer services that our consumers expect.

Chairman TAUZIN. There you go, Mr. Chairman. I have found you unanimous consensus.

My work is done. Thank you very much.

Mr. STEARNS. I thank the chairman. Mr. John? Oh, no, he is not here. Mr. Doyle?

Mr. DOYLE. Thank you, Mr. Chairman. Boy, I sure hate to rain on the parade here. And I think this has been a good discussion, and a helpful one. But let us all remember here, too, that sitting before us are representatives of Fortune 100 companies, and I think that in an ongoing basis we also need to hear from consumers and from small businesses, because I think they face some different problems complying with and adhering to privacy policies than some of these companies here, who have vastly greater resources. And that needs to be kept in mind.

Mr. Misener, at Amazon.com you sell videos, right?

Mr. MISENER. Yes, sir.

Mr. DOYLE. We have a Federal law that if I walk into Blockbuster and buy a video, they are not allowed to keep a record of what kind of videos I am buying. Now, obviously that law doesn't apply to Amazon.com online, because you keep records of what kind of videos your customers buy?

Mr. MISENER. We keep those records in the ordinary course of our business, which is a specific exclusion in that law.

Mr. DOYLE. Yes, exactly. So in that respect, your online service is treated somewhat differently than an off-line service.

Mr. MISENER. Well, if off-line services were using those records in the ordinary course of their business like we do, they also could keep those records.

Mr. DOYLE. But Blockbuster could never disclose or keep records of anybody's purchases, I am saying. You could share that information, could you not?

Mr. MISENER. Let me be clear on a couple things.

Mr. DOYLE. Sure.

Mr. MISENER. First of all, we would be delighted to be in the Fortune 100. We would actually be delighted to be in the Fortune 500.

Tune in this time next year. But we are fully compliant with that video restriction law that you mentioned, because we do use those in the ordinary course of business. We do not reveal—repeat, do not reveal—that information to third parties at all.

Mr. DOYLE. But you do that voluntarily, is what I am saying. There is no law requiring you to do that. You do that as a matter of policy.

Mr. MISENER. I think it could be argued that that law applies to us. But we are responding to what our customers demand. If we

did that, we would lose customers, and therefore, because our customers want it, and because we are pro-privacy, we do it. And so therefore, the market forces are forcing us to do this. Just like keeping our prices low and providing a high level of convenience, we are providing a level of privacy protection that consumers demand.

Mr. DOYLE. Yes. And I guess the point I am trying to—and it is certainly not an attack against Amazon.com—but we have all kinds of vendors and entities out there that all have varying degrees of privacy policies, and do things that they are not really required to do. You do it because it is good for your customers. And that is what we are hoping for, that there isn't going to be a need for heavy regulation because the industry understands that that is the way to go.

But I can tell you that most consumers don't have a clue how data is being collected on them. They don't understand what a cookie is; they don't know, when they are surfing the web, what is happening to them. Trust me, they don't.

And I guess it doesn't bother me so much in the retail end. I mean, I go to Giant Eagle and I have got my little Advantage Card, and you know, I swipe that across the deal and I get some discounts for doing it. But it also allows that supermarket to track what I am buying, and make sure that the stuff I want is there. I think it is helpful that we don't get junk mail, if people know what our preferences are. So I see tremendous benefits from it.

But I also see the tremendous potential for abuse, especially in things like medical records and issues of personal behavior, where consumers have the right to expect that those types of information aren't being shared with anyone, and that when you are dealing with vendors—I know you say some of your vendors have the same privacy policies that you do. I just don't understand what the enforcement mechanisms are. How do you know they are not violating their own policy?

So I guess, you know, we struggle with these things. And it is politically unpopular to want to do anything against the Internet, because it is such a sexy new thing, and you know, everybody wants to be seen as high-tech up here on this panel. But I think there are some real concerns, and we appreciate your input at these hearings. And I think we have a long way to go, Mr. Chairman, to hear from many different groups, so that when we do fashion legislation we do it thoughtfully.

But I appreciate your testimony today.

Mr. STEARNS. I thank the gentleman. The gentleman from Illinois, Mr. Shimkus?

Mr. SHIMKUS. Thank you, Mr. Chairman. And I am glad my colleague Diana DeGette here, because I used her phrase, since you mentioned it, in hearings earlier this year about individuals not——

Ms. DEGETTE. See that you get it right.

Mr. SHIMKUS. Yes, she is concerned that I am using some of her quotations. But how much individuals—we don't understand the benefit we have from some information sharing. And although we want to find out the benefits to you from having good, strict policies.

And I was just interested here in how much you actually are using the information in product-specifics at P&G, personalized beauty care products to individuals, and the information and the like.

I want to boil it down a little simpler, in the debates that we use here and the terminology that we use here in legislating in this arena, and get a few comments. And I want to address questions on this opt-in/opt-out aspect, because in some aspects, when people order from Amazon.com—which we have done—it is almost implied that you are opting in, because you are providing the information that they have to send you the product. And then there may be some other boxes to put. And I am not sure if it is a total requirement to fill in all the boxes before you get an order processed—versus an opt-out provision which would say, I want to buy your product. But I don't want you to get any more information on me. All I want to do is purchase your product, and opt out—do not use this for anything else.

We also use here in Washington-speak the telephone directory as an opt-out system that works. We wouldn't have a telephone directory that worked if everyone had to call in and say, yes, I really want my phone number listed in a directory. But we do know that if you call, you will get an unlisted number. For a price, as I'm being corrected. But that is a price that some people are willing to pay.

So I would like to have your comments on how the whole debate on opt-in/opt-out affects you individually as you do this planning, and how you are going to respond to whatever it is that we end up doing. And I would do it the same way—actually, yes, let's just go the way the chairman did at the table. And if you don't want to add, then you can just pass.

Ms. PEARSON. Opt-in versus opt-out, from a business perspective it boils down to choice, and what is the right amount of choice to provide the consumer when you are dealing with a consumer? And that is really, if you are a customer-centric business, is what is the expectation of that consumer, and what is going to result in a better environment, a more trusted relationship? Because I want to continue my relationship with that consumer. And so sometimes you market and you use opt-in.

Particularly for us, in e-mail solicitations, we will only send out e-mails if somebody has opted in or we have a prior existing business relationship, where there is no surprise when you are going to get that e-mail.

Sometimes it make a lot of sense to do opt-out, because all we are going to do is, if you are not going to check here, we are going to take advantage of your not opting out and send you an additional piece of literature about that IBM Aptiva. And we want to do that. And there is really very little harm that comes from doing that.

So sometimes it is opt-in, sometimes it is opt-out. And then the debate becomes, should there be a national requirement as to one certain level? And should you impose that on every kind of business decisionmaking, or how you interact with the consumer? That is the real question.

Ms. HOURIGAN. I would agree with Ms. Pearson's statements, and also add: it comes down to prominence, and making sure that you are doing it in a way that is understandable to the customer.

I think—wearing my consumer hat for a minute—I have seen it done, opt-in and opt-out, done in very positive ways, and in very sort of, you know, less than satisfactory ways. So again, I think the important concept here is choice, and prominence, and presenting it in a conspicuous and understandable way.

Mr. SMITH. I would second the call for the fact that the prominence and the clarity of the choice is more important than what the default is. We use a system in Proctor & Gamble, and we are moving it to universality in our company. But we ask, you know, would you like to have other offers from this brand? Would you like to have other offers from other Proctor & Gamble brands? Would you like to have offers from other reputable companies who are partners? And so we get kind of a hierarchy of choices for our consumers.

Mr. MISENER. My wife is from the North Hills, just north of Pittsburgh. And we go up to the area frequently. And we have a Giant-Eagle card. And I can assure you, down at the bottom of that application form—I don't recall it exactly. But I am sure that there is a little check box that says that you can probably opt out of getting solicitations based on your purchases there. Small print, down at the bottom, didn't pay attention to at the time, probably wouldn't care much about it.

On Amazon.com's site, when we talk about information with one of our affiliates—for example, ToysRUs.com for certain toys deliveries—we actually have a little cartoon picture prominently displayed on the site, which shows Geoffrey the Giraffe, the Toys R Us giraffe, sitting in an Amazon.com box. Now, that little picture makes it crystal clear to our customers, without having read a long privacy policy or read the fine print at the bottom of the page, that Amazon.com is going to be delivering a Toys R Us product. Real simple. That is meaningful choice, in our view.

And so yes, as I mentioned before, we provide opt-in choice for any kind of sharing with our affiliates, and we don't share any information, period, with any non-affiliated third parties. But when there is that choice, we want to make it meaningful choice, so that customers and consumers actually understand what is going on. Frankly, Geoffrey sitting in the box makes a lot more sense to consumers than small type at the bottom of a form.

Mr. JOHNSON. There is not a whole lot I can add to what has already been said. With respect to our business, our business is very different from Amazon's in that we are a well established direct merchant. The opt-in aspects of communication via the Internet is only relatively new to us in the history of our business.

It would be fair to say that in transacting our business, to an earlier point raised, there is a certain amount of information that is required. But with respect to opt-in versus opt-out, depending on online or off-line aspects of our business, we comply with what we believe to be the expectations of our customers. So with respect to our Internet business, our communications via e-mail, it is very clearly opt-in. On the catalogue mailing side of our business, we certainly give our customers choice there as well, making sure that

they know that if they want to limit that sharing of their name and address with like-minded companies, that that option is available to them.

Mr. SHIMKUS. Thank you very much. I yield back.

Mr. STEARNS. The gentleman's time has expired. The gentlelady from California, Ms. Harman?

Ms. HARMAN. Thank you, Mr. Chairman. I have an opening statement which I would like to submit for the record.

Mr. STEARNS. By unanimous consent, so ordered.

Ms. HARMAN. And I would mention that in it, I attach an interesting op-ed that appeared earlier this week in the New York Times, authored by Peter Wallison, a friend of mine who is a former counsel to President Reagan, in which Wallison points out the difficulties of opt-in and what it would do to the financial community. I thought it was very interesting to read that author make that point.

At any rate, I have appreciated the testimony of the witnesses, and would like to declare, at least for myself, that these are the good guys. You are all good guys. And I congratulate you on being sensitive to privacy concerns.

My question, Mr. Chairman—maybe it is for you and the committee, more than it is for our panel—is what about the bad guys? What about the people who are not sitting here, who don't think that privacy and protecting our privacy matters?

And interestingly, I understand that today's Industry Standard reports a list of sites with the greatest concentration—not absolute numbers, but the greatest concentration—of teen users. I raise this because I know we are all concerned with teenagers. As a mother of two of them myself, I certainly am. But none of those people are sitting here. Let me just read this list: Teen.com, TeenPeople.com, Katrillion.com, SparkNotes.com, BadAssBuddy—I'm sure we would love that one—dot-com, Blink182.com, CoolQuiz.com, TeenMag.com, TeenChat.com, and Seventeen.com. Some of these sound pretty antiseptic. There is one word I read that I am sure we are all going to now check out.

But at any rate, here is the Katrillionsite, just so you know. Katrillion is reported to be an entertainment and gossip portal. Here is what it says on the site: "By using this site, you agree to the terms and conditions outlined below. If you do not agree to these terms and conditions, please do not use this site."

Okay, good.

"We reserve the right to change, modify, add, or remove portions of these terms at any time, whenever we want. If you continue to use the site after we have posted changes to the terms, it means you have accepted those terms."

Now, if you are 16 or 17, you won't even read this. But if you read this, and then you logged on to the site—at least the way I understand this, and I realize my mind is not as agile as my children's—the way I understand this, they can do whatever they want.

So I would at least postulate that Katrillion would not be a good guy in the way that you are, because I don't think that is what you would do.

I want to ask the panel, Mr. Chairman, I really have only one question, what do you have to say about this kind of information? Your kids, presumably, or your nieces and nephews, or your brothers and sisters, or teenagers that you know, are logging on to these sites much more than they are having anything to do with you. And what advice do you have for us about this kind of stuff?

Ms. PEARSON. I have a 9-year-old daughter who, when she is old enough to go on the web by herself—which is when she is going to be 18——

Ms. HARMAN. Good luck.

Ms. PEARSON. I would be—yes, you're right. I am very concerned about that, as a mother. And there are not only privacy issues raised in what you said, Ms. Harman. There are many other issues raised. It is absolutely critical that we educate our children, particularly those who are old enough to be on their own on the web, about what to look for. There is absolutely no reason that a teenager should not be looking for some sort of privacy policy or seal, or other kind of indicator of what is good for them.

But we all know that they are going to go wherever they shouldn't go anyway. Those sites, no matter what they say, are still bound by laws. And they still should be bound by industry practices, so that if they are not doing what they say they are doing, they ought to be prosecuted, and there should be enforcement. If they are doing something misleading, collecting information and abusing that information to hurt a child, they should be prosecuted to the fullest extent of the law. And there are laws that can get you there.

If they are a bad guy and they disregard industry practices and they disregard existing law, then they are a bad guy, period. And I am afraid that a law or industry practice, whatever that is, is still going to lead to having some bad guys out there. So for us, it fundamentally becomes an issue of education. Educating our kids, and making sure parents are involved with the children.

Ms. HARMAN. Other comments?

Ms. HOURIGAN. I would just add, with respect to that site, and actually just general commercial web sites, with respect to privacy and consumers, education is absolutely key. Technology is challenging; you know, I have to read new articles on a daily basis to keep up. And so making education part of any comprehensive privacy solution is appropriate.

I would also say, with respect to the bad guys, you lose customers if you don't treat them well. From a large company's perspective, if we lose a customer, it is hard for us to get them back. And so that really drives us to say, hey, this is incredibly important, and we need to respect our customers and respect their preferences.

Mr. SMITH. I think empowering consumers to make decisions is important. And that probably means parents need to step up to the responsibility of training their kids. Some interesting data: 82 percent of people on the web have seen privacy statements. That is going up. Sixty-seven percent say they sometimes or always read them. I suspect that that is an overstatement, to a degree. But you know, they are aware of them. Fifty-six percent of people say that privacy statements are important. And the great thing about the

web is that you are always one click away from—you know, if you make the consumer mad, boom, hit the "Back" button, and you are absolutely out of there.

So I think the issue is how do we enable people to understand privacy policies and make choices?

Ms. HARMAN. Well, my time is up, Mr. Chairman. Any other comments?

Mr. STEARNS. Sure.

Ms. HARMAN. I thank you. I just want to state for the record that I am quite dubious about whether Federal legislation will work here, with the exception of some bright lines around medical and financial privacy, personal privacy. I think the rest of it might better be handled by responsible actors in the industry. But having said that, there are irresponsible actors. And particularly when they interact with teenagers, whom—I would volunteer, as one parent who attempts to be responsible—who are difficult to fathom.

I think we are at risk, and I don't know what the answer is. And it sounds good to say we should all make good choices. Yes. I agree. Mr. Chairman, I think you should make good choices, and I hope you have a better ability than I do to understand what is in your kids' head, and to guide them perfectly.

But I think, as a society, we are at risk here. And I don't know whether we are yet finding the best tools to help overworked parents deal with kids. And I would welcome some enlightenment here. And I hope that all of you, in your role as parents, keep thinking about this, because we certainly have a lot of work to do.

Thank you, Mr. Chairman.

Mr. STEARNS. I thank the gentlelady. The gentleman from New Hampshire, Mr. Bass?

Mr. BASS. Thank you, Mr. Chairman. Two or three observations about what I have heard in the last hour or so. First of all, only an absolute dyed-in-the-wool retail salesperson could characterize an unsolicited e-mail offer or advertisement as a benefit. It is the computer equivalent to seeing somebody drive up your driveway in a car full of clothes or something in the back and saying, "Oh, boy, this is just what I have been waiting for all morning long!" I am not sure how popular that really is.

Second, I myself, and my wife, buy products online, and from nothing but very reputable firms. And yet I receive on average 4 or 5 solicitations on my e-mail address to consolidate my loans, to travel to faraway places, to make money fast. All you have to do is click this button and you're rich. And I don't know how it ever got there, and I think that is part of—by illustration at least—what we are facing here today. I am not—these are companies like yours.

The third observation I have is that we really are—I as a consumer, am presumably at least moderately knowledgeable—really don't know what to look for. You mentioned, Ms. Pearson, that we need to educate our children about what to look for. Well, if we don't know what to look for, then it is hard to educate anybody else.

My question for you folks, if you wish to answer—you can or not—is, you have high standards. I think, Mr. Misener, you men-

tioned that you sell your list to other people that have the same standards that you have.

Mr. MISENER. I did not say that.

Mr. BASS. Oh, somebody else did.

Mr. MISENER. We absolutely do not sell our list.

Mr. BASS. Okay, Land's End, Mr. Johnson did. To use the analogy of whispering in a circle, after a while the message may begin to get indistinct. What happens to the lists that you sell to them, and then they sell, and so forth and so on? I guess you said your clients have the same standards that you do. That is a requirement internally, is that correct?

Mr. JOHNSON. That is correct.

Mr. BASS. And is there any way that that information can be abused by your clients?

Mr. JOHNSON. We take a number of measures to protect against that. As I stated in my testimony, it is for one-time usage only, and that is by a contractual agreement. We also, in managing that process, we plant what we call our decoys. I myself am a decoy on that list. So we track usage by those companies, and we track it very closely, so that we can ensure that it is a one-time usage, and that the usage of it is as was stated in the original agreement.

Mr. BASS. And you are adequately protected should there be abuse? You could seek civil action of some sort?

Mr. JOHNSON. Absolutely. Yes.

Mr. BASS. All right. Let's see. Does your commitment to consumer privacy extend to sites that might link to or from your sites? In other words, there might be people that are linking. Can you control the ability for other sites to link to your site, or vice versa? Does that make sense, or not?

Mr. SMITH. The answer is you really can't control who can link to your site. On our sites, if you are moving out of a Proctor & Gamble site somewhere else that we have linked, there is a notification that you are leaving the Proctor & Gamble area, and that different policies may pertain.

Mr. BASS. Okay. I have no further questions, Mr. Chairman.

Mr. STEARNS. Thank you.

Ms. PEARSON. Can I make one point on education?

Mr. BASS. Sure.

Ms. PEARSON. Mr. Bass, you mentioned that it would be great to know what to look for. And I just want to come back to that and say that this education, this need for further education, is a bipartisan, it is an industry-government—we all need to work together on education.

And I would commend the Federal Trade Commission for providing a certain level of education. I would say FTC.gov and the material there is what every consumer ought to take a look at. I think any number of our companies has been involved in this kind of effort. Trustee.org, BBBOnLine.org, and a few other organizations such as UnderstandingPrivacy.org, the web site for the Privacy Leadership Initiative, all have information about what a consumer could look for. And any kind of assistance you can provide in this committee to highlight the availability of those materials, or to suggest further activities, or to encourage the Federal Trade

Commission to encourage that kind of activity, I think would be appreciated and welcome by the American public.

Mr. STEARNS. I thank the gentleman. The gentlelady from Colorado, Ms. DeGette?

Ms. DEGETTE. Thank you, Mr. Chairman. I would like to add my thanks for having this series of hearings, and also to announce that at the conclusion we are going to pull my original comment I made at the first hearing, and whoever paraphrased it the most closely is going to win a prize.

Mr. STEARNS. Skiing in Aspen.

Ms. DEGETTE. Skiing in Aspen? Yeah, okay, I'll work on that.

I want to go back to something Ms. Harman talked about and others touched on. And Ms. Pearson, you were just talking about it briefly, which is, how do we educate consumers? Because I hear everybody up here talking. I hear Ms. Hourigan talk about what they do internally to help identify consumer preferences, and to help their customers, and so on. And I hear others talking about what happens online.

And I guess my question—I think we all know consumers are really not educated at all as to what is going on with their personal information. Some of it, we might agree with the uses, some we may not. But consumers don't know—despite disclaimers, despite privacy policies on web sites, despite some kind of education effort. So my question to you is, do you think industry has any obligation to find some way, jointly or separately, to increase consumer education, and what would that be? Beyond what we are doing now, because what we are doing now is not educating consumers. Anyone?

Mr. SMITH. Well, I think industry does sense the responsibility to communicate and improve the education. A number of firms in industry and leading trade associations about a year ago created the Privacy Leadership Initiative. A key element of that work was consumer education. We have developed, and will soon launch, a web campaign with privacy tips for consumers.

Ms. DEGETTE. And how is that going to be disseminated to consumers, so that they can actually know?

Mr. SMITH. As they visit web sites, a banner ad will pop up with a privacy tip, that explains a privacy practice. You know, how to create a good password, for example. And then have the URL to visit the Privacy Leadership site for additional tips.

Ms. DEGETTE. And how widely is that going to be disseminated?

Mr. SMITH. I don't have specific impression estimates at the moment. But the members of the Internet Advertising Bureau have very generously committed to run these ads on a pro bono basis.

Ms. DEGETTE. Anyone else with thoughts on that?

Ms. HOURIGAN. I would just add a couple of comments. The concept that Trustee, which is one of these seal programs, recently announced regarding labeling, so you would basically develop a label for a particular practice on a web site—I think that will go to at least alleviating some of the burden on a customer to go through and read a privacy statement and understand. And hopefully, again, that will serve to—it will be a little more transparent to the customer. I think that is an interesting concept. I am not sure what the status of that initiative is, however.

The other thing I would mention is the introduction of the platform for privacy preferences, or P3P, which will be built into Internet Explorer 6.0. What I think we hope for is this becomes almost a transparent issue for customers, and they become familiar with it, because it is built into their browser, they can select their preferences, and basically it will be an effort for the browser to look in course and communicate that information back to them.

Ms. DEGETTE. Well, you know, I appreciate these answers. But as you yourself can realize, they are not very specific or broad. And so my suggestion to the industry—I know we have many representatives here today—would be you start to think about these things on a much broader scale, especially because we are all loath to have over-reaching government regulations, which means there is a big responsibility for companies.

And let me follow up, because the title of this hearing is "How do Businesses Use Customer Information: Is the Customer's Privacy Protected?" This hearing, and your testimony, is not just about online privacy, but privacy in general. And I am wondering if any of you can talk about whether you think standards for privacy for data that is not online should be different than online data. And if not, how do we deal with that? All of your answers were related to Internet privacy.

Mr. MISENER. Ms. DeGette, thank you. As I mentioned in my testimony, we strongly believe it ought to apply equally off-line as to online, for a variety of reasons, not the least of which that so few transactions and so few consumers actually are online.

My wife and I purchased a small $15 space heater a few months back, and inside was a warranty registration card. In the card, in filling it out in pencil, they wanted me to list our household income, where we took our last vacation, whether or not we read the Bible, and whether or not someone in the household has prostate problems.

Now, I assure you this information is far, far more sensitive than any information Amazon.com collects. It would be patently unfair to consumers—to consumers—not to address that issue, as well as the online issue.

Ms. DEGETTE. Right. And how do we address that issue without passing a law?

Mr. MISENER. All I am suggesting is that when we think through whether or not the market is taking care of it, whether or not there are real problems out there, they ought to be addressed equally on- and off-line.

Ms. DEGETTE. Thank you.

Ms. PEARSON. Ms. DeGette, my answer, and I think a number of the other answers, were that our practices apply online, off-line, no matter where we're getting information, throughout our companies. And there is sort of, within my company there is an equal level of protection for information.

I think in terms of how to handle these issues, I would suggest focus first on that information that is the most sensitive. For example, medical information. You know, we have strongly supported Federal-level legislation on medical, very sensitive information for a long time, and we are very happy that there has been some activ-

ity and movement in that area, to create Federal-level protections. Those are absolutely sensitive information.

Ms. DEGETTE. Thank you. Thank you, Mr. Chairman.

Mr. STEARNS. I thank the gentlelady. The gentleman from Oregon, Mr. Walden?

Mr. WALDEN. Thank you very much, Mr. Chairman. I have a couple of questions. I want to follow up on something Mr. Bass said I think is of interest to me. I get those same sort of junk e-mails, if you will allow me to use that term.

And I guess I am probably not unlike a lot of other consumers who want to be able to respond and tell somebody no, stop sending that to me, get me off your list. And yet I am sort of fearful that if I do, I may actually end up on more lists. You know, because I have heard that if you open some of those, then you really connect, and away you go. So I think as you wrestle with that one, I would be interested in your comments.

I would also be interested in your comments on international standards, because the Internet is so ubiquitous. We run into this issue with other Internet-related problems—we can establish a standard here, but what are you facing in other countries, in terms of privacy? You talk about State pre-emption. What are you facing in terms of other countries?

And then I guess another question I would have for you is have you analyzed these off-line laws on privacy—you talked about the collection of data there—to see how and if they should be applied to online data collection and privacy standards? I understand what Mr. Doyle was saying regarding the rental of movies, and I understand Amazon, you know, abides by that same sort of carve-out in the statute. But are there other off-line—if we are going to treat everybody equally—statutes regarding privacy that we need to follow?

So I will throw it open to you for your responses.

Ms. PEARSON. Let me address the international question, Mr. Walden. I will let my colleagues address the question of unsolicited commercial e-mail.

We operate in 160 countries, and so we have deep experience handling information all over the world, both on our own behalf, as well as on behalf of many companies and organizations. And I can tell you, similar to what Mr. Swift said in his oral remarks, that many countries have data protection, data privacy legislation. Most others do not. And it is a concept that is kind of foreign and not really developed in many parts of the world, particularly in Asia-Pacific and in Latin America.

I can tell you that we provide the same level of protection throughout the world, and that the requirements that are imposed on us in Europe, of course we comply with. But I cannot, as Mr. Swift said, say to you that we are providing any greater level of protection to the average European citizen by virtue of that. Sure, we have to go through some more administrative steps. We have to have a few more managers doing different things. But I have to tell you that we are probably more conscious of the issue and more innovative in the United States than we are almost at any other place.

This is where we have developed our policies. This is where we have a chief privacy officer. This is where we have engaged in industry leadership activities, to try to move forward on the issue. So, that is my comment on the international side.

Mr. WALDEN. Anyone else on any of those three points?

Ms. HOURIGAN. I would add to the complexity of dealing with the international standards. And it is not just the privacy laws; it is what the consumer expectation is. And that varies dramatically by country.

We continue to actually look at the options available to us, to determine what the most appropriate approach is, given that we are in over 200 countries. But very, very complex and very complicated.

Mr. SMITH. I think the international requirements—and just looking at the European Commission principles—I think align very well with principles of the OECD of 10 or 15 years ago, of the FTC fair information practices. When I began working in privacy about 2 years ago, it seemed to me that those principles were how I wanted to be treated, or how I would want my children to be treated.

So I think it is fairly easy, on a principle standpoint, to get to appropriate principles. The question really is in the administration. And if I were to test—the question is whether the process benefits the consumer or not. You know, I think there is a fair amount of the process that benefits lawyers and paper manufacturers, and does darn little for the consumer.

Mr. WALDEN. Mr. Misener?

Mr. MISENER. I might take up the question of unsolicited e-mail. First of all, Amazon.com never, ever sends unsolicited e-mail to those who are not customers. And as far as e-mails marketing certain products, at Amazon.com we provide a menu of some 150-plus different categories that you can go in and select, choose opt-in to receiving e-mails on specific items of interest.

Mr. WALDEN. Right. Different deal.

Mr. MISENER. So, for example, I have mine set up to send me information on history books and jazz music, two interests of mine. This is the kind of thing that is being addressed, by this committee and also the Judiciary Committee in the House, and also in the Senate as well, in the context of spam. And we are trying to get at—as I understand, the industry and Congress are trying to get at these nasty e-mails that we receive from random places about all sorts of get-rich-quick schemes and such. And so hopefully those can be addressed. But I think those are outside the context of these privacy sorts of discussions.

Mr. WALDEN. Yes, to an extent. Although it seems like if you respond to some of those, they are able to apparently take your data and go and send it elsewhere, it seems like. I don't know.

Do you have a comment on the off-line laws, privacy laws that are out there, versus online?

Mr. MISENER. Yes, and it is a huge topic. There are several trade associations, the ITI in particular, who has done an extensive listing of the extant off-line privacy protection laws. And so we would be happy to provide that to you. It is actually quite long in different areas. And they tend to be targeted, as Ms. Pearson was saying earlier, to things like medical privacy and children's privacy—things that are the most sensitive kinds of issues.

Mr. WALDEN. Okay, that would be helpful. Thank you.

Mr. JOHNSON. Just with respect to the off-line versus online issue, I don't believe that our customers view themselves as off-line customers or online customers. They are Land's End customers, and they have expectations of us. And it is so critical for us to maintain that relationship with that customer, and do everything in our power to further the customer's interest and make sure that we are not in any way, shape, or form risking that wonderful relationship we have with our customers. So I don't see the consumer as necessarily differentiating between an online versus off-line.

Just one other point with respect to off-line. As we consider off-line, I think we do need to be very careful about the implications that off-line legislation potentially has for very small companies, very small retailers that are not involved in the online arena. You know, it potentially has an impact on the many very small companies that do business in this country.

Mr. WALDEN. Thank you, Mr. Chairman.

Mr. STEARNS. I thank the gentleman. Mr. Terry is going to pass?

Mr. TERRY. Yes, I could be redundant and repetitive, but I will relieve you of that.

Mr. STEARNS. Okay. Before I let you go, if any other member has a quick question—I had a quick one. Mr. Swift, you mentioned in your opening testimony about the recent European legislation dealing with information privacy on the Internet, and how you said it was "unimaginable burdens" for a company like yours, with no substantive benefits. But I understand you have joined the safe harbor decision, to have Proctor & Gamble go into safe harbors. Is that a compromise? Or are you—tell me your reasoning on that.

Mr. SWIFT. Well, the issue is really not safe harbor. The issue really is not the European Data Directive. The issue is that the Data Directive required 15 European countries to create their own privacy legislation that comported with the Directive. Twelve of the 15 have. The three others are in the process.

So as a company that operates, and has data, and has employees and consumers in all 15 of those countries, I need to obey those laws. And the issue of the Data Directive really was to facilitate transfer of data within European countries. So we observe the European laws and have no problem transferring data there.

The issue is that I need to be able to move employee data anywhere in the world. I may choose to move employee data from the U.S. to Europe for processing, or from——

Mr. STEARNS. By joining the safe harbors, you are complying with the European Union Internet privacy.

Mr. SWIFT. I am. But it is one choice. In non-U.S. countries, I have contracts. In other words, if it is going from Europe to Japan, I have to have a contract. And what I have chosen for the United States, for administrative efficiency, really what I have done is I have created 400 contracts between my P&G entities. Which means that I don't have a contract when I transfer a specific type of data. I have freedom to transmit any type of data within our corporate entities.

Mr. STEARNS. So you did it for self-survival?

Mr. SMITH. Well, it is obey the law, and what seems to be the most efficient or effective way to obey the law.

And honestly, what I have found as I have gotten into privacy, half of my time needs to be spent in making sure that our information practices enable our business practices, not impede them. You know, our lawyers, the easy answer from a lawyer in Europe is, "Well, don't move the data out of Europe." But that is not the right thing for the business.

So I have to continually look at how can we do what is right for the consumer, what is right for the business, and at the same time obey the law? And in this case, I had no choice by to do 400 internal contracts, and uncountable external contracts.

Mr. STEARNS. Now, Ms. Pearson, IBM, I understand, has not signed up. Why haven't you signed up?

Ms. PEARSON. Not yet. As you can tell, this stuff is mind-numbingly complex. It can get really complex. We similarly have operations everywhere in Europe, and we move data globally. So we have come up with a fairly complex—and I will spare you the details—way of complying with the European law.

The safe harbor framework is a framework of principles that very importantly, between the U.S. and the EU, there is a handshake that says, the EU says, okay, if U.S. companies comply with that framework and use U.S. mechanisms, including self-regulatory mechanisms, you are okay for Europe. That is a very important statement. And we believe in the safe harbor; I support it in principle.

It may or may not be the right fit for our operations, because we are this big enterprise that is really complex. I think it is an ideal mechanism——

Mr. STEARNS. Proctor & Gamble is pretty big and complex.

Ms. PEARSON. And actually we are still looking at the safe harbor for our web operations, because that is an area where it makes a lot of sense, since we do use a self-regulatory trust-mark, the Trustee program, for our web. So we actually may still enroll in it for that purpose. And I think it makes a lot of sense for companies who are doing business over the web, in particular small- or medium-sized.

Mr. STEARNS. And of course GM, I understand, has not signed up either. And you are a big company, too, and complex.

Ms. HOURIGAN. That we are.

Mr. STEARNS. So why haven't you signed up?

Ms. HOURIGAN. We actually are—safe harbor is one of the alternatives we are looking at. As of today, we comply with the European laws; therefore I don't have an issue with transferring information within the EU countries.

Mr. STEARNS. But if the data base is outside of Europe, you would have to comply.

Ms. HOURIGAN. That is correct. And we actually, as we speak, are investigating all of our options available. And we will make a decision in the near term.

Mr. STEARNS. Just tell me why you haven't joined. What is there, the part about the European legislation that you don't like? What specifically is preventing you from joining? Last year, I think the Clinton administration had negotiated 30 large companies. And you folks weren't one of them. What is there specifically why you didn't buy?

Ms. HOURIGAN. I don't think there is any specific part that we dislike. I think it is the challenge of—we are looking at—again, we operate in over 200 countries. So the EU is one issue, but because we are global we are trying to come up with a global solution. And to the extent that—we may decide to take advantage of safe harbor.

Mr. STEARNS. Is there anything that Congress could do to make this simpler for companies like yourself?

Ms. HOURIGAN. I don't think so.

Ms. PEARSON. The issue is, we have a European law, and we are complying with a European law, in various ways. And the safe harbor framework is one way to do it.

Mr. STEARNS. But you have not signed up, and I just want to know why IBM and General Motors have not signed up. What specifically is the reason?

Ms. PEARSON. There are other ways of complying with the European law. So the safe harbor is 1 of 3 or 4 or 5 ways of achieving compliance with that law.

Mr. STEARNS. I am not saying you should necessarily. I am just curious.

Ms. PEARSON. And so, at this point, I think what help the government, from the U.S. side, could do is to keep actively engaged with Europe in oversight capacity and dialog capacity, to make sure that U.S. companies are treated similarly with European companies with respect to how this law is implemented. Because it is a very important issue going forward.

Mr. STEARNS. Anyone else like to mention anything else? And then if any other member would like to add another question, I would be glad to welcome that. Mr. Doyle?

Ms. HOURIGAN. I will add one—I'm sorry—one very brief comment. And that is when safe harbor was negotiated, as you all know, there was a carve-out for financial services. We have a tremendous presence, with our GMAC operations, in Europe. And that is one thing that we are looking at, because that is not included in safe harbor.

Mr. STEARNS. Okay. Mr. Misener?

Mr. MISENER. Mr. Chairman, thank you for this question. And actually it gives us an opportunity to hopefully clear up some of the misconceptions that have been produced in the press recently.

Safe harbor does not imply one way or another necessarily compliance with the underlying national privacy laws in European countries. We are fully compliant with all the national privacy laws there that govern the transfer of information in and out of the European economic area. However, we have not sought safe harbor protection; we have not yet been convinced of the value of the safe harbor in itself. Yet we are fully compliant with the national laws.

And so it is not the same to say that we are not complying or interested in complying.

Mr. STEARNS. Well, you were just saying that if you had signed a legal document, then the enforcement mechanism in the European Union would apply to you. And right now——

Mr. MISENER. That is correct.

Mr. STEARNS. [continuing] that is what it sounds like you are worried about.

Mr. MISENER. Well, I am not sure we are worried, actually, Mr. Chairman.

Mr. STEARNS. Not worried—it's a word. But I mean, it is another ambiguous set of circumstances that you don't know the implication of, and yet you are complying.

Mr. MISENER. I think that is fair to say. We are just not yet convinced of the value of seeking safe harbor treatment per se. Although, again, I clarify that we are fully compliant with the national laws in Europe, and therefore don't necessarily need to attain that safe harbor protection.

Mr. STEARNS. Okay. Mr. Doyle?

Mr. DOYLE. Yes, thank you. Just one quick follow-up. Just before you leave—and if you could take off your company hats and just be citizens and consumers, we won't hold you responsible for anything you say.

Mr. STEARNS. Just forget the camera.

Mr. SMITH. Oh, sure.

Mr. DOYLE. We will never tell anyone else what you said.

Mr. SMITH. You will protect our privacy, right?

Mr. DOYLE. You have got complete privacy here.

But just to help us with this, you know, these computers, they are getting faster every day. They store more information. It is scary to think 5 years from now how quick they will be, and how rapidly we will be able to collect and disseminate information. What scares you, or concerns you, as a private citizen, about the ability that many people are going to have to collect and disseminate information on just about everything? I mean, what scares you when you just think as a private citizen about this technology, and what is the potential for abuse?

I mean, I get these things on my—maybe because we are in politics. But I think we get them all the time. "You can spy on your neighbors and friends," you know, just sign up here and you can learn anything you want to learn about your political opponents. And I have always been tempted to click on that.

But I haven't. But think—I mean, 5, 10 years from now, given what is happening in this technology, what really scares you about this ability to collect all this information on one another?

Mr. SMITH. I think to me the question is, where does harm occur? If someone takes a communication out of a mailbox that has a person's Social Security number, and from that steals a person's identity, that is concerning. And you know, that has been possible as long as there have been mailboxes and Social Security numbers. And if we find that there are elements that, you know, at some level of frequency create harm, then we have got to break the code. We have got to stop the pipe on that.

Typically, that is not where companies in commerce are. I mean, our consumers vote for us every day, and we are trying the best we can to get them information. And those are the things where we don't want to break the code or break the bank.

Mr. DOYLE. But just as a citizen.

Mr. SMITH. I don't want my identity stolen. I don't want my credit cards stolen. I appreciate it when people inform me of practices that can help me for those things not to happen.

I think, you know, some of the software that is being developed that will give us more choices about the data that we give up on the Internet all make good sense. You know, if you don't want people to have the answers to what is on the warranty card information, don't do it. You know, most of the stuff that you get on the web, it has an unsubscribe at the bottom. Let's help people hit the unsubscribes. And my bet is that most of the things that we are most concerned about would be something that may be facilitated to a degree by technology. But it is, you know, how do you stop a criminal from doing a criminal act?

Ms. HOURIGAN. I would just add to the concept of identity theft, I have had two people very close to me undergo—it has just been an absolute nightmare for them. And it has got such a tremendous ripple effect, sweeping consequences. And it really requires a tremendous amount on a consumer to try and rectify a wrong that was completely outside his or her control.

Mr. DOYLE. We are getting called to vote.

Mr. STEARNS. Yes. Anyone else?

Mr. MISENER. Well, Mr. Doyle, very quickly, before I was brainwashed in law school I was an electrical engineer and a computer scientist. And I do have an appreciation for those huge data bases that are out there, that you mentioned. Those exist quite distinct from the Internet. The Internet is a communications medium, as we all understand. But those data bases are also connected to a typist who actually took that little warranty card asking about the prostate problems in my family, and typed it into those data bases.

I think what the concern is, as a citizen, is the type of information that we are talking about here. I don't care if someone knows that I bought that pan at Amazon.com. I really don't care. I do care, however, about medical records, financial information, information about young children, those sorts of things. And those things deserve a higher level of scrutiny and protection.

Mr. JOHNSON. I agree absolutely with what everyone here has said. As a consumer, as a citizen, the technology itself doesn't scare me a bit. A concern, though, as a consumer is with respect to, as Mr. Misener stated, financial information, health care information, which is dealt with separately and is protected. So the technology itself and the communication mediums and whatnot really don't frighten me.

Mr. DOYLE. Thank you all.

Mr. STEARNS. Ms. DeGette? Mr. Towns?

Mr. TOWNS. Hearing all of this—and believe me, there are a lot of problems—you still feel that we should not do anything? The Congress?

Mr. MISENER. Do I feel that you should not do anything? I don't think legislation is inherently necessary, as I mentioned before, because I think companies are being forced to address these issues head-on, or they are not going to survive. These are the kinds of issues that we must do, simply to please our customers and to survive in the marketplace.

So no, Mr. Towns, I don't believe that legislation is inherently necessary. But if there is a belief that there is a need to address specific areas of information—for example, financial or medical or children's information—I think that strong arguments could be

made to go after those specific types of information, as opposed to the medium through which they are collected.

Mr. SMITH. And one of the things that I would urge is that we start from where the harm is. You know, with Graham-Leach-Bliley, all of us have had our mailboxes full of disclaimers that are too long to read and incapable of being misunderstood. And the reason was that we didn't look at where the harm was, but we looked at a type of data. And I think we need to find where the difficulty is and then address that difficulty, rather than to take a blanket approach on a specific type of data. As important as it is.

Ms. PEARSON. I hope you will pass new privacy legislation, at the right time, on the right subject. I am not smart enough today to tell you exactly what it is, but I hope we can work together to find it.

Ms. HOURIGAN. And I would also urge, if that were to take place, industry appreciates being involved. And there are a lot of practical complexities associated with this issue. And so we would appreciate having our input heard.

Mr. TOWNS. Mr. Johnson?

Mr. JOHNSON. I concur with Mr. Misener. I believe the vast majority of companies doing business today are doing everything in their power to protect their relationships with the consumer. And I would just caution that we not do something that inhibits our ability to ultimately serve our customers and provide benefits and valued services and products to them. As Ms. DeGette said earlier, how do we target the bad guys, the very few that raise these kinds of issues? I don't know that I have answers for that, but I am not convinced necessarily that legislation is going to be successful at doing it.

Mr. TOWNS. Thank you very much, Mr. Chairman.

Mr. STEARNS. I thank my ranking member. We have finished with panel No. 1. We have been called to vote. So it is probably appropriate to reconvene after these—I think we have two votes. So we will do that, which would be—we have 10 minutes left on this, and then 5, 15. So hopefully we will reconvene in about 15, 20 minutes. And so I thank panel No. 1, and if panel No. 2 will hold, we will be right with you.

[Recess.]

Mr. STEARNS. The committee will reconvene, and we will have panel No. 2. And we thank you for waiting.

We have Jennifer Barrett, Chief Privacy Officer of Acxiom. And we have Mr. John Ford, Chief Policy Officer, Equifax, Incorporated. And Ms. Deborah Zuccarini, Executive Vice President and Chief Marketing Officer of Experian. Welcome to you.

And Ms. Barrett, if you don't mind, we will have your opening statement.

STATEMENTS OF JENNIFER T. BARRETT, CHIEF PRIVACY OFFICER, ACXIOM; JOHN A. FORD, CHIEF PRIVACY OFFICER, EQUIFAX, INC.; AND DEBORAH ZUCCARINI, EXECUTIVE VICE PRESIDENT AND CHIEF MARKETING OFFICER, EXPERIAN MARKETING SOLUTIONS

Ms. BARRETT. Thank you, Chairman Stearns, Ranking Member Towns. For more than 30 years, Acxiom has been a leaders in re-

sponsibly providing innovative data management services to a who's who of America's leading companies. And we do it in a way that goes beyond what is required by law or self-regulation, in order to respect consumer privacy.

Acxiom believes that any use of information to defraud or discriminate must be illegal. At the same time, we strongly believe in a balanced approach to the collection and use of information. The free flow of information we enjoy today has greatly contributed to our Nation's economic growth and stability. Consumers have greater choice and variety. Goods and services cost less. And transactions are completed faster and more easily.

It takes much more than just instinct to recognize what consumers want. One hundred years ago, the local shopkeeper knew just what his customers bought, but knew them also personally, knew how they spent their time, and he knew their family.

Today's consumers are as likely to shop through a catalogue or over the Internet as they are in a store. The business-to-consumer relationship requires new information tools. Acxiom helps businesses recognize and engage consumers who likely have the greatest need for what they are selling. Our operations include two distinct components: data base management services, and information products.

Specialized computer services represent 90 percent of our revenue, and help companies manage their customer information. This includes keeping up-to-date customer records in order to ensure opt-in or opt-out requests are properly honored, and saving companies millions of dollars when unwanted duplicate promotions are eliminated.

The other 10 percent of our business comes from a separate line of information products. These allow businesses to improve their relationship with consumers, irrespective of whether they live in a city or in a rural area, whether they are a parent or an elderly shopper. For example, a major kitchen and bath store used our product to reach households with elderly patrons likely interested in learning more about their new senior product line, including shower grips, bath stools, and large-print clocks.

The real winner in the use of information to engage in the consumer is the consumer. To fit all the pieces of the marketplace together that we have learned and heard about today, I have provided a chart on page six of my testimony, and as well on the easel you see over here to your right. Point A on the chart represents the consumer, who expects to complete transactions quickly, obtain the best prices, and choose from the widest variety of products and services. At point B, we find the business, who responds to these expectations by understanding their customers and their market. To do this, they need information beyond that collected during a sale. For example, the characteristics of a household, such as are there elderly consumers in the home?

This information is available from two points, or from two sources: point C, which is directly from another merchant; or point D, from information compilers such as Acxiom.

For example, our customer enhancement products give businesses the demographic, lifestyle and interest information they need to understand their customers and the market. And our com-

piled list products provide access to likely new consumers who would like to be customers.

We compile or acquire the relevant information from a variety of sources, points E and F on the chart, and aggregate this data by household. We compile public records and we acquire self-reported and other general information directly from companies that sell products and services to consumers, and who offer a third-party opt-out.

We only receive general summary information, indicating probable interest or lifestyle data. We do not have detailed data about individual transactions. Acxiom only sells data to qualified businesses, under contract for specific use. We do not sell data on one individual or a household, and we do not sell data to the general public. Our information products help businesses and consumers fill in some of the missing pieces in today's relationship gap.

We are also very proud of our ingrained culture of respect for privacy. Since we do not have a relationship with the consumer, we ask our customers to refer any consumer to us who inquires about our data. We have posted a privacy policy on our web site since 1997, and we maintain a consumer care department to handle inquiries. We also provide an opt-out to all marketing products through our web site and via a toll-free hot line.

We have consistently not only met but exceeded all requirements placed on us by law and industry self-regulation, by establishing our own even more restrictive policies.

In closing, there are a few things that I would like to add that we do not do. Acxiom does not have one big data base containing data on every individual. Instead, we have many different information products designed to meet the various business needs of our customers. The information we provide cannot be used for decisions of credit, insurance, or employment. And we do not sell Social Security numbers, credit or other detailed personal financial information that could be used to steal someone's identity.

In short, we are committed as business leaders and consumers ourselves to protecting consumer privacy.

Mr. Chairman, on behalf of our more than 5,000 associates, I wish to thank you for the thoughtful approach which your subcommittee continues to use in studying this very important issue. And we appreciate the opportunity to be here.

[The prepared statement of Jenniffer T. Barrett follows:]

PREPARED STATEMENT OF JENNIFER BARRETT, CHIEF PRIVACY OFFICER, ACXIOM CORPORATION

INTRODUCTION

Chairman Stearns, Ranking Member Towns, and members of the Subcommittee, thank you for the opportunity to participate in this timely hearing and to share Acxiom Corporation's perspective on how the current flow of information powerfully underpins the vibrancy of the new American economy.

As your Subcommittee continues to explore the issue of privacy in the responsible manner that this series of hearings evidences, we strongly support the concept that a balanced approach to the use of information must be achieved. We believe that inappropriate use of information to defraud or discriminate against consumers should be illegal, as it is already in most situations. Furthermore, the relatively free flow of information we find today in the U.S. has significantly contributed to our nation's economic growth and stability by enhancing variety in consumer goods and services, by facilitating lower domestic prices as compared to foreign markets, and

by accelerating the speed and ease with which transactions can be completed. We believe that it is imperative that consumers be protected from fraud and discrimination while the benefits to both consumers and businesses are preserved.

When privacy laws and implementing regulations overreach, the results can be devastating: legitimate businesses suffer irreversible damage, and consumers unintentionally lose many advantages. It is our hope that by sharing our story with you—as well as by separating information myths from reality—we will aid you in evaluating an appropriate legislative direction.

ABOUT ACXIOM CORPORATION

Founded in 1969, Acxiom Corporation has more than thirty years experience in customer data management services, technology leadership, and awareness of and sensitivity to consumer and business privacy concerns. We are based in Little Rock, Arkansas, with operations throughout the United States, Europe, and Asia. Our annual revenues approach $1 billion. Our company has over 5,000 employees worldwide: with over 2,800 of them working in Arkansas, almost 1,000 in Illinois, more than 200 in California, and 170 in Arizona.

Acxiom's business includes two distinct components: database managment services and information products.

Database Management Services

Acxiom's database management services, which represent ninety percent of the company's revenue, include a wide array of leading technologies and specialized computer services. These services help large companies improve and boost customer loyalty, retention, and market share by making accurate "customer recognition" possible across multiple lines of business and across multiple points of sale, including the Internet, call centers, and retail outlets.

Customer recognition is critical to delivering an exceptional initial customer experience, retaining that customer, honoring consumer preferences about how personal information is used, and improving business profitability. Although e-commerce has increased consumer product availability, it also has made customer recognition more difficult.

Acxiom's database management services assist companies in better managing their customer information to address this need. For example, it is not uncommon for a company's databases to contain several different names and address variations for the same person. We provide services that will accurately recognize a particular individual. Our services can save a company millions of dollars when, for example, unwanted duplicate catalogs or other mailings are eliminated. Moreover, we assist companies maintain up-to-date records to ensure that their customers' opt-in or opt-out requests are properly honored.

Informational Products

Acxiom also offers a complementary line of information products that represent the remaining ten percent of our gross revenues. Our InfoBase information products allow businesses to make smarter and faster strategic decisions, streamline customer communication at every point of contact (Website, telephone, store, wireless, and more), personalize and target various communications, and strengthen relationships with their customers. The majority of our testimony today further explains these products.

THE ECONOMIC NEED FOR ACXIOM'S INFORMATION PRODUCTS

Acxiom's information products help fill an important gap in today's business to consumer relationship. Think back to 1901. The local shop owner knew his customers and his market well. The shop owner was familiar with what they bought, what they liked to do, how they spent their time and something about their family. Today, large and small businesses are trying to achieve the same level of knowledge about their customers' interests and needs as the small shop owner enjoyed a hundred years ago. This need for knowledge is not new. In the current environment, however, with customers shopping remotely via the Internet, on the phone and through catalogs, securing information about customers that allows companies to better serve them is more difficult to accomplish.

In our information-based economy, companies grow by exceeding consumer expectations with unparalleled products and services of the highest quality. Despite technological advances, businesses do not instinctively know what their customers want and need. Acxiom's information products provide the additional knowledge necessary for businesses across diverse industry sectors to stay in touch with and to satisfy their customers in order to achieve profitability and market growth.

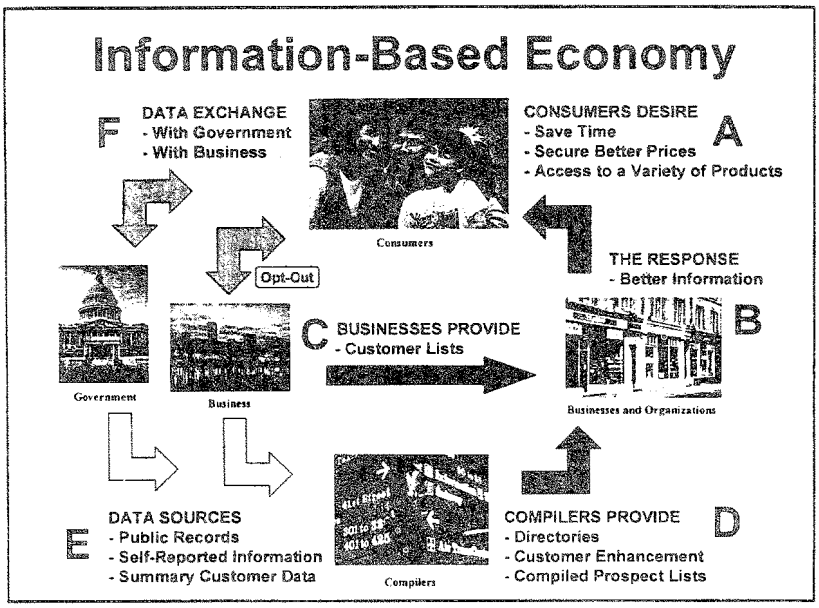
Our role is to help businesses systematically recognize and engage consumers who, with the aid of our information products, are believed to be those with a likely interest or need for their products, or services. While changing technology, such as the Internet, has largely reshaped the mechanics of how commerce is conducted, the basic strategy of marketing remains constant—the operational need to focus a company's marketing efforts on those most likely to have an interest or need in their products or services.

With Acxiom's information products, companies have been able to accomplish goals such as:

- A kitchen and bath store used age to recognize their elderly customers in order to offer them a new senior-lifestyle product line of kitchen and bath enhancements—shower grips, bath stools, large print stove dials, large print clocks, and better grip door-knob covers.
- A bookstore used age to recognize the right audience to promote a new line of large-type books, including large-print Bibles.
- A major publisher used the knowledge of which subscribers had younger children in the household to promote a new publication for kids, which was co-branded with Crayola.
- A computer software company used the knowledge that certain households owned a computer to promote in-home access to educational software.
- A computer manufacturer employed information on households that did not have computers to offer a special purchase price in order to encourage the use of educational and in-home financial management software.
- A retailer used the knowledge about which customers in their area had swimming pools to offer special products and prices for pool toys and supplies, as well as an inventory management resource to determine how much merchandise of this type to stock in each local store.
- A local bass fishing supply store launched a catalog to reach customers outside their store trading area by knowing which households had a passion for their specialty—fishing.
- A small tool company expanded their customer base by mailing catalogs to professionals interested in power tools at a discounted price.
- A local day care program promoted a special offer to single moms in their local community.
- A literacy program in English was focused on reaching non-English speaking families in rural areas.

Without the use of our information products, each of the businesses in the preceding examples would have been less effective in communicating with their existing and potential customers. Consequently, the real winner in the use of information to engage consumers is the consumer.

The following chart has been provided to assist the Subcommittee in understanding the information marketplace from a more macro perspective, as well as the key role that Acxiom plays in this interchange.



Consumers expect to complete transactions quickly, obtain the best price possible, and be able to choose from a wide variety of products and services—as reflected in point A on the chart. Businesses—point B on the chart—respond to the expectations by working hard to understand their customers and their market. To do this effectively, they need information beyond that collected during the sale. If the information cannot be collected directly from the consumer, then it is available from two sources—either directly from other merchants—point C—or from information compilers, including Acxiom—point D. Information compilers use public information, primarily obtained from the government, or in some cases collected from other businesses—point E—that obtain the information through their relationship with the consumer—point F.

Information Product Development

Acxiom begins its information product development with the identification of a marketplace need. For example, in order to achieve growth and product objectives, businesses may need to know something about the characteristics of a household. Is it a single adult household, or is it a married couple? Do they have children, and if so, are they small children, teenagers, or college aged? Other relevant characteristics might include whether the household has an interest in certain hobbies, such as cooking or gardening, or participates in certain activities—do they play tennis, golf, or both? Such characteristics are extremely relevant in determining whether a consumer in that household may want to learn more about a product or service.

Once a particular information need by business has been identified, Acxiom compiles or acquires the relevant information from a variety of sources and aggregates it by household. This is a complex process which varies on a case-by-case basis. However, it is important to emphasize that in all such efforts, any data collected is general in nature and *not specific* to transactions or events. It *does not* include details on specific actions that an individual has taken, confidential medical information, or specific information regarding children. Once the data is collected, Acxiom must clean, integrate, and package the information into a product that meets the marketing needs and information demands of businesses. We invest significant time and resources in developing these products. Finally, a successful information product provides Acxiom's customers with enough of the right information to solve their specific business problem or need.

Acxiom does not sell data on one individual or one household at a time. We do not sell information to the general public. Information is sold by the thousands of elements or records to qualified businesses. We perform a credit check on all pro-

spective customers. Once we are satisfied about our customer's qualifications, we require them to sign a contract that binds their use of the information acquired from us for specifically articulated purposes. Acxiom and our customers typically enter into long-term contracts—one, three, or five years—for use of a particular information product.

Categories of Acxiom's Information Products

Our information product offerings provide needed intelligence for three primary functions: (1) our directory products provide telephone information necessary to locate, verify or contact consumers by phone; (2) our enhancement products provide the information businesses need to better understand their customers and their market; and (3) our list products provide access to consumers who are potential future customers. As mentioned earlier, these products comprise about ten percent of Acxiom's gross revenues.

Directory Products: Containing name, address, and telephone number, Acxiom's line of directory products are compiled primarily from the white and yellow pages of published U.S. and Canadian telephone directories—5,900 different directories in the U.S. alone.

For example, we license some of our directory products to companies as an inexpensive form of directory assistance and to Websites that provide free nationwide directory assistance. These Web-based directories benefit consumers in many ways, such as providing help in finding friends or family members with whom individuals may have lost touch.

In all our directory products, Acxiom respects a consumer's choice regarding unpublished numbers. The names and numbers we include in these widely-used directories are derived only from those consumers who have elected to have their number made publicly available by their local telephone carrier. Moreover, for consumers who contact us in writing, through our Website, or by calling our toll-free Consumer Hotline, Acxiom offers the option to opt-out of this service if, for instance, the consumer wants to keep a published number in the local printed telephone book, but not have it available on a Web-based directory.

Enhancement Products: Acxiom also offers businesses lifestyle, demographic, and interest data on their customers to enhance the company's knowledge about their customers and provide a better understanding of their customer's desires, needs, and changing characteristics. Demographic data includes such information as the makeup of the household—single, married, with or without children. Lifestyle data might include information such as home ownership, retirement status, or average income strata of the neighborhood. Interest information would identify a passion for cooking or golfing.

This demographic, lifestyle and interest information is added to a company's already-existing customer files, known as "response lists." The information is general in nature. We do not provide detailed transactional information. We license enhancement information to qualified businesses through a menu-oriented approach. Businesses license only the data needed for a particular business decision or process. In many cases, we have pre-packaged information groups to meet common or recurring business needs for specific industries.

How might a business use enhancement information? First, it is used to better understand the interests and needs of current customers. Second, enhancement data is employed to identify the best market segments for up-selling or cross-selling particular products. Finally, demographic, lifestyle, or interest data can help identify characteristics common in a business' best customers in order to target similarly-situated prospective customers who may be more likely to have an interest or need for the company's products or services.

List Products: Acxiom offers prospect lists as a third type of information product. These lists are built from a variety of information sources, and represent broad coverage of the population. Prospect lists, which contain much of the same information contained in our enhancement products (including demographic, lifestyle, and interest information), differ from a particular company's response lists in so far as they contain information about consumers with whom the company has had no prior relationship.

Prospect lists allow businesses to take the information about their best customers and apply that knowledge to selecting likely households of potential new customers. Acxiom sells prospect lists to businesses, not-for-profit organizations, and political parties and candidates.

Data Sources for Acxiom's Information Products

The information we acquire to build our information products is obtained from three general types of sources—public information, self-reported information, and

summary customer information from companies who have consumers as customers. Acxiom compiles or acquires this information from several hundred carefully chosen sources with whom we have cultivated and maintained long-term contractual relationships.

Public Information: Public records and publicly-available information are the foundation of Acxiom's information products. The types of data that Acxiom acquires or compiles include: telephone directories and other types of publicly-available directories, property records, and other state and county public records. This information provides the basic names, addresses, and general demographic information, such as home ownership, profession, and the age of members of a household.

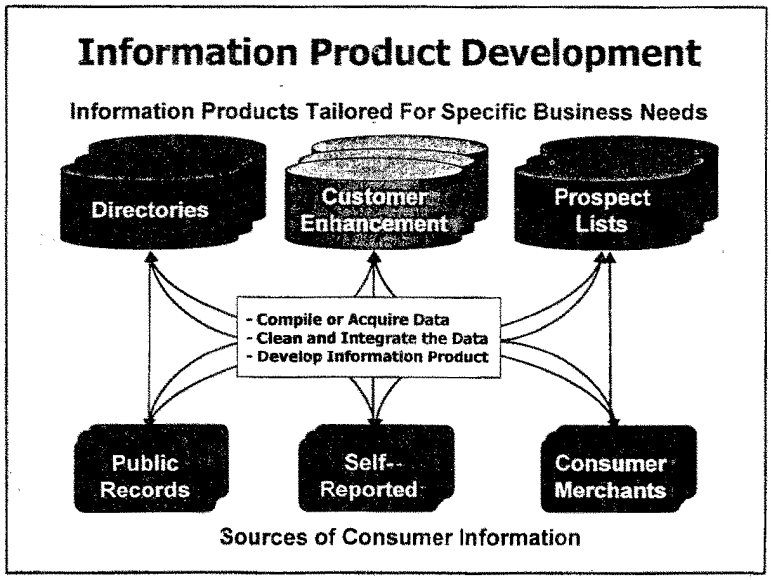
Self-Reported Information: Surveys and questionnaires are an additional source for demographic information and provide much of the lifestyle and interest information we acquire. Consumers are asked to voluntarily complete surveys, such as those contained on warranty cards, from a variety of companies asking for specific information. In these cases, the consumer is customarily provided the opportunity to opt-out of further use of the information beyond that of the company conducting the survey.

Information from Merchants: Acxiom acquires some information directly from companies who sell products and services to consumers. In these instances, we ensure that consumers have received an opportunity to opt-out of their information being shared with a third party, such as Acxiom. Also, we only receive very general summary information that indicates possible lifestyle or interest data. We never receive detailed transaction information. Rather, general information that we acquire is used to extrapolate lifestyle or interest characteristics. For example, knowing that certain households subscribe to a magazine on golf would indicate that those households have an interest in golf, just as the fact that those households ordered that subscription from a Website would indicate that they are Web-enabled.

In some cases, Acxiom compiles information directly from the source, such as the telephone directory and the property records. In other cases, Acxiom acquires this information from other reputable information providers, who perform the original compilation, or we acquire the information directly from the business holding the relationship with the consumer. Acxiom carefully screens all information providers and businesses from which we receive information to assure that the information has been legally obtained and is appropriate for the intended use.

The information Acxiom collects on an individual or a household is always incomplete. Acxiom does not have information on every individual, and we do not have the same kind of information on all individuals. For example, we may or may not have the telephone number of a household. We may or may not have property information. We may or may not have lifestyle or interest information. Our goal as an information provider is to provide sufficient coverage of various data elements to meet the market needs for that particular piece of information.

The following chart summarizes the process Acxiom uses to take information from a variety of sources and to develop specific information products designed to meet the business needs of various markets.



RESPECTING CONSUMER PRIVACY

Acxiom has a long-standing tradition and engrained culture of respecting consumer privacy in the development and marketing of our information products. I have been employed by Acxiom for 27 years, and I have been responsible for privacy oversight since 1990. Privacy has been my full-time job over the past three years.

Since Acxiom does not have a customer relationship with individual consumers, we do not routinely have direct contact with the individuals whose data we hold. Therefore, we ask our customers to refer any individual consumer to Acxiom who may inquire about the sources of data they have obtained from us. Since 1997, we have posted our privacy policy on our Website, before it was an established and common practice. Acxiom maintains a Consumer Care Department to handle consumer inquiries. We also provide consumers who contact us in writing, through our Website, or by calling our toll-free Consumer Hotline the option to opt-out of all of our marketing products.

Our privacy policy is designed to adhere to all Federal, State, and local laws and regulations on the use of personal information. In addition, Acxiom follows the industry self-regulatory guidelines of a number of trade associations in which we are active members, including the Direct Marketing Association, the Online Privacy Alliance, and the Individual Reference Services Group. These guidelines include posting a notice that describes what data we collect, how we use it, to whom we sell it, as well as what choices consumers have about the use of that data. We recently certified under the European Union Safe Harbor and have applied for and are in the final stages of being certified for the BBBOnline Seal.

Acxiom is also an active member of the Privacy Leadership Initiative and the Coalition for Sensible Public Record Access. We believe that consumers should be educated about how businesses use information. To that end, we publish a booklet, entitled "*What Every Consumer Should Know About the Use of Their Individual Information*," which is available both on our Website and upon written or telephone request.

Acxiom takes its responsibility toward protecting consumer information seriously. Beyond the industry accepted guidelines which we follow, we have also established our own guidelines which are more restrictive than industry standards. For example, we do not provide Social Security numbers or other personally identifiable information about children in any of our products. Moreover, we only capture the specific information required to meet our customers' information needs, discarding the remaining data, when we compile information from public records. These voluntary information practices are internally and externally audited on a regular basis.

MYTHS ABOUT INFORMATION PROVIDERS

With the full picture of Acxiom's business operations now outlined to better explain what we do, I believe it is important to close by reiterating for you what Acxiom does not do. Over the years, a number of myths have developed about the information industry that require clarification. Please allow me to set the record straight:

- Acxiom *does not* have one big database that contains detailed information about all individuals. Instead, we have many databases developed and tailored to meet the specific needs of our business customers—entities that are carefully screened and with whom we have legally-enforceable contractual commitments.
- Acxiom *does not* provide information on a particular individual to the public. The information we sell is provided only to qualified businesses for specific legitimate business purposes. I cannot call up from our databases a detailed dossier on any of you, let alone me.
- The information we provide *cannot be used,* according to existing law, for decisions of credit, insurance or employment. These activities are regulated by the Fair Credit Reporting Act and such uses are prohibited under our contracts.
- Acxiom *does not* contribute to the nation's identity theft problem. We do not sell Social Security numbers or credit card numbers to anyone, nor do we sell credit or other detailed personal financial information that could be used to steal someone's identity.
- Acxiom *does not* develop any information products containing sensitive information. We define sensitive information as personal information about children, medical information, and detailed financial information. The only exception to this would be a situation where the consumer has opted-in to volunteer such information for distribution or where the information may be a part of the public record.
- Acxiom *does not* sell detailed or specific transaction-related information on individuals or households, such as what purchases an individual made on the Web or what Web sites they visited. The information we provide is general in nature and not specific to an individual purchase or transaction. For marketing purposes, businesses need information about the household, not the specific individuals comprising the household.

Mr. Chairman, on behalf of our over 5,000 associates, Acxiom appreciates the opportunity to appear today to share with the Subcommittee a detailed overview of our core business operations. We also wish to thank you, Mr. Chairman, for the deliberative and thorough approach with which this committee has studied the appropriate and inappropriate uses of information in our economy. Acxiom is available to provide any additional information the Subcommittee may request.

Mr. STEARNS. Thank you.

Mr. Ford, your opening statement?

STATEMENT OF JOHN A. FORD

Mr. FORD. Mr. Chairman, Mr. Towns, counsel. I am John Ford—that's Chief Privacy Officer, sir—for Equifax. I thank you for this opportunity to summarize the written statement that Equifax submitted for the record.

I am going to talk a bit fast so that I can stay within the time limit, so let me get straight to the point. Equifax's view is that personal information for marketing purposes provides important benefits to consumers, to businesses, and to our economy, and that the potential privacy risks or harm arising from these uses are small, are already subject to effective privacy safeguards, and need not be subject to further privacy regulation.

Founded in 1899, Equifax is the oldest and the largest of the credit reporting companies in the United States. Our activities here are regulated under the Fair Credit Reporting Act and related State statutes. As a separate company, Equifax Direct Marketing Solutions maintains one of the largest marketing data bases in the world.

I want to emphasize that our consumer reporting data base is entirely separate and distinct from our direct marketing data bases—physically, managerially, operationally. As a responsible steward of information, Equifax is committed to the fair and ethical use of data, the free flow of information, self-regulatory initiatives, and to forging effective information privacy solutions.

When assessing privacy risks and harms, at least four key topics, I think, are relevant. First is source: is the source of the information reputable and reliable? Second, content: is the data base information aggregated, anonymous, or is it personally identifiable, is it sensitive?

Use: will the information be used to benefit the individual, or does its use put the individual at risk for adverse action? And finally, privacy protections: are there adequate privacy protections already in place?

The answers to all of these questions, I believe, support the conclusion that the privacy risk or harm from direct marketing is minimal, the benefits are substantial, and little basis exists for more governmental regulation.

Regarding sources, at Equifax much of the personally identifiable information provided for marketing purposes is consumer self-reported data. Third-party data sources include public record repositories, other government agencies that provide, for example, hunting or fishing license information, and other types of reputable sources using publicly available data, such as telephone white pages or other directories and exchanges, and census data.

Regarding content, our marketing data bases contain primarily information that is predictive: that is, information that describes the characteristics that people who live in a particular geographic area are likely to have. Even when the information is more granular, it typically describes buying characteristics of a household, not necessarily of a specific individual.

We do collect sensitive, personally identifiable information, but only when the consumer has voluntarily provided it. The personal information we obtain for marketing purposes is not used for risk assessment; rather, the information is used to efficiently shape and deliver the kinds of offers an individual is most likely to want. As a result of direct marketing, consumers become aware of new products and services, businesses sell more products more cost-effectively, and the economy grows.

Some have suggested that such target marketing provides some consumers advantages over others who do not receive the direct mail offer. The fact is, businesses have a limited number of dollars to support marketing campaigns. It only makes sense that businesses would seek to achieve the best return possible by focusing on those most likely to respond. Similarly, Members of Congress do not mail campaign solicitations to every constituent, but usually only to those who have given before or who are more likely to respond.

As I said at the outset, Equifax has adopted privacy protections for marketing data that are appropriate to the use and any potential harm. For example, we have always contractually prohibited our customers from using our data base for individual lookup, and our system has no delivery mechanism for a customer to query the

data base based on a name. Data collection or exchange, rather, is done in batch mode, usually computer to computer or via mag tape, making review by an individual virtually impossible.

In sum, direct marketing is a societal and economic good. Overall, the process is profitable, efficient, and benign. The concept is consumer-oriented and privacy-sensitive.

In closing, I want to congratulate you, Mr. Chairman and the subcommittee, for your leadership in this privacy arena. We look forward to working with you so that the marketplace might achieve the further synergies that can arise from a better understanding, and a greater appreciation, of the important benefits of direct marketing.

[The prepared statement of John A. Ford follows:]

PREPARED STATEMENT OF JOHN A. FORD, CHIEF PRIVACY OFFICER, EQUIFAX INC.

I. INTRODUCTION

Mr. Chairman and members of the Subcommittee, I am John Ford, Chief Privacy Officer for Equifax. I want to congratulate you, Mr. Chairman, and the members of your subcommittee and its excellent staff for the thoughtful and thorough manner in which your subcommittee is reviewing the information privacy issue.

In this statement, I briefly describe Equifax; our commitment to protecting consumer privacy; and, from the Equifax perspective, the sources, content, and uses of marketing data and the associated protections.

I recognize that the primary purpose of this hearing is to better understand the flow of data in the marketing process. Beyond that, it is my intent to discuss this process in a way that supports Equifax's view that personal information, when collected and used for marketing purposes, provides important benefits to consumers, to businesses, and to our economy. Further, the potential privacy risks and harm arising from the use of personal information for marketing purposes are small, are already subject to effective privacy safeguards, and need not be subject to further privacy regulation at this time.

II. EQUIFAX

A. Background

Founded in 1899, Equifax is the oldest and largest of the companies that provide consumer information for credit and other risk assessment decisions. These activities are regulated under the Fair Credit Reporting Act and dozens of related state statutes. In addition, Equifax Direct Marketing Solutions, formerly part of Polk, maintains the largest marketing database of lifestyle and compiled data in the world. At the outset, I want to emphasize that the personally identifiable information in our consumer-reporting database is entirely separate and distinct from information contained in our marketing databases. In fact, the databases are managed by totally separate Equifax companies.

B. Equifax's Longstanding Commitment to Privacy

More than a decade ago, Equifax was one of the first U.S. companies to develop and adopt a meaningful privacy policy. At the risk of sounding flippant, we were privacy before privacy was cool. As a responsible steward of information, our commitment to consumer privacy has remained steadfast. We remain committed to three Core Values, described in greater detail in Section III.D. below, in order to foster the fair and ethical use of data. We support self-regulatory and marketplace initiatives to balance the substantial benefits of the free flow of information and the legitimate concerns about the privacy of personally identifiable data, and we seek opportunities to work with governments, consumers, and businesses to forge effective solutions to the complex information-use issues worldwide.

C. Equifax Products

Equifax believes that the marketplace can offer solutions that enlighten, enable and empower our customers and consumers to address effectively some of the information-use issues today. So, increasingly, Equifax is providing products directly to consumers to assist them in understanding their credit profiles and to empower them to fight identity theft and manage their fiscal health. For example—

- Equifax's **Score Power** gives consumers access to their actual BEACON credit score, along with an explanation of how that score is used by credit grantors and recommendations about how consumers may "improve" their score.
- Equifax's **Credit Profile** gives consumers online access to the information in their Equifax credit file.
- Equifax's **Credit Watch** provides consumers with online notification of changes to their credit file within twenty-four hours, thereby providing early detection of potential identity theft.
- Equifax's **eIDverifier** patent-pending product permits consumers to use information from their consumer credit report to establish their identity virtually instantaneously in a reliable and secure manner so that they can obtain products and services online. This service deters identity theft and fosters trust in e-commerce by facilitating an electronic handshake between a known consumer and the online vendor. Subsequent online transactions are encrypted, further enhancing trust and protection.

III. MARKETING AND PRIVACY

When assessing privacy risks and harm, at least four key topics are relevant:

1. **Source.** Is the source of the information reputable and does it put the record subject on notice that information is being collected?
2. **Content.** What is the content of the information—is the information aggregated or anonymous or is it personally identifiable and is it sensitive?
3. **Use.** Will the information be used to benefit the individual or does its use put the individual at risk for adverse, substantive action?
4. **Privacy Protections.** Are there privacy protections already in place to eliminate or minimize privacy risks?

When it comes to marketing, the answers to all of these questions, I believe, support the reasonable conclusion that the privacy risk or harm is minimal; the benefits to consumers, to business and to the economy are substantial; and little basis for more governmental regulation exists.

A. Sources

Equifax provides information to its customers for marketing purposes from the following categories of data sources, in conjunction with an array of analytical services.

At Equifax, most of the personally identifiable information provided for marketing purposes comes from consumer self-reported data. For example, Equifax's Survey of America and our online survey, RightOffers (www.rightoffers.com), give millions of consumers an opportunity to voluntarily provide information about themselves and the members of their households and to exercise choice in what kind of marketing offers they receive. Another source of self-reported data included in the Equifax marketing databases is product registration cards. On a voluntary basis, consumers may provide information about themselves by responding to lifestyle or buying preference questions included on paper product registration cards, electronic product registrations, or Internet registrations.

Other data sources include third-party data sources such as public record repositories and other government agency data sources (e.g., land records, certain license information such as hunting and fishing licenses, and census data), and other types of reputable third-party sources including those using publicly-available data such as telephone white pages or other directories and exchanges.

In essence, our databases contain personal or aggregated data about individuals or households that is self-reported, inferred through sophisticated modeling procedures, or obtained from reputable third-party sources, including public record or publicly-available sources.

B. Content

The vast majority of information held by Equifax for marketing purposes is not personally identifiable information. Information does not have to be personally identifiable in order to be useful to marketers. Marketers can successfully market their products and services on the basis of predictive, aggregated information. Whether aggregated data is appended to a client's list of names and addresses, offered with our analytical services, or used to develop a predictive model, the key purpose is to help companies market products and services to consumers who are likely to be interested. This information is very valuable to marketers for predicting consumer spending patterns. Consumers benefit because they receive only those offers in which they are likely to have an interest. What's the result: Consumers become aware of new products and services, businesses sell more products more cost-effectively and the economy grows.

While the vast majority of information held by Equifax in its marketing databases is not personally identifiable, as indicated above, Equifax's marketing databases do contain some name and address information. Naturally, marketers must have name and address information in order to communicate their offers directly to consumers. It is important to note, however, that the information included within the Equifax marketing databases is not organized so as to be readily and easily retrievable by personal identifiers (i.e., name and address).

Our marketing databases contain primarily information that is predictive, psychodemographic information, such as "Zip+4" information—that is, information that describes the characteristics that people who live in a particular geographic area are likely to have, including lifestyle information.

Even when the information is more granular than geographic "Zip+4" type information, the information describes some of the buying characteristics of a household, not necessarily of a specific individual. For example, both the Survey of America and the online RightOffers survey provide information that is used as a primary source for our marketing databases. Both surveys ask participating consumers to provide certain lifestyle information, including information about their leisure activities and hobbies and those of the other members of their household, as well their preferences regarding product categories and/or brands. In addition, consumers are asked to provide certain demographic information such as marital status, month and year of birth, and occupation for household members. The information collected from surveys is used in the aggregate to better understand consumer preferences, past buying behavior, and responsiveness to direct marketing.

Finally, in no instance is the marketing information we collect sensitive personally identifiable information, unless the consumer has voluntarily provided it. Even then, the data pertain to the household, not an individual.

C. Uses

It is very important to emphasize that personal information obtained for marketing purposes is not used for risk assessment purposes. Marketing data is not used to make decisions about whether an individual obtains or retains a job, insurance, or a government license or benefit. Instead, the information is used merely for the purpose of efficiently shaping the kinds of offers an individual receives.

Some have suggested that such target marketing provides some consumers with an advantage over others who do not receive the direct mail offer. It only makes sense that businesses would seek to cost-effectively align their marketing with their markets, achieving the best return possible by focusing on those most likely to respond. The simple truth is that businesses have a limited number of dollars to support marketing campaigns. Similarly, Members of Congress do not mail campaign solicitations to every constituent but only to those in their party and then only to those who have given before or who are more likely to respond. In order to accomplish this goal, marketers must direct their offers based upon their understanding of consumers' buying preferences and willingness to respond to direct marketing offers. Individual consumers are not excluded from receiving marketing offers.

In addition, marketers constantly refine their marketing campaigns based upon changes in consumer spending patterns and other predictive information. As a result, the audience to which a marketer directs its offers may change. Furthermore, consumers who express an interest in a particular product or service directly to a marketer are likely to be included in marketing campaigns.

D. Privacy Protections

As I said at the outset, Equifax has adopted privacy protections for marketing data that are appropriate to the use and any potential harm. For example, we provide consumers with notice and opportunities to opt-out (sometimes opt-in) of Equifax's use of marketing information. We provide consumers who participate in our Survey of America with the opportunity to specify on the Survey how their information may be used. Survey of America participants may opt-out of receiving future survey questionnaires, product samples and coupons in the mail, or coupons and special offers from companies via email by simply checking the appropriate boxes on the Survey form. Consumers who complete product registration cards have similar opt-out opportunities.

In addition, in some situations, we provide opt-in opportunities. At our "RightOffers" website, not only do we provide consumers with the ability to opt-in to marketing uses by selecting only those categories of offers that they want to receive, but we have implemented a double opt-in system. Under that system, once we receive a completed RightOffers survey, we send the consumer an email asking the consumer to confirm his/her desire to receive offers. Furthermore, RightOffer

participants may update their information by revisiting the site and are free to unsubscribe at any time.

We also employ state-of-the-art technology to help ensure data integrity and security. In addition, our customers are prohibited from using our marketing databases for individual look-up purposes. We have always contractually prohibited our customers from using our database for this purpose. Furthermore, we have designed our system so that we have no delivery mechanism for a customer to query the database based on a name; therefore, no individual look up is offered or feasible.

Further, Equifax provides consumers with meaningful and practicable privacy protections through our compliance with a variety of self-regulatory programs providing consumer rights and redress. We adhere to the self-regulatory principles of organizations such as the BBBOnline Privacy Seal program, the Online Privacy Alliance, and the Direct Marketing Association.

Finally, in consultation with renowned privacy expert, Dr. Alan Westin, Equifax conducts privacy audits of our procedures as well as our products and services to ensure high standards of privacy protection and, in fact, to provide a value-added quality.

All of these protections are consistent with Equifax's three Core Values to which we adhere in order to protect the fair and ethical use of data—

Core Value I: Equifax is committed to the ethical use of data and to maintaining the highest standards of consumer information privacy. We adhere, therefore, to a meaningful set of self-regulatory privacy principles enterprise wide.

- Responding to and anticipating evolving technology and changing societal demands, we have managed sensitive consumer data in an ethical manner for more than 100 years, earning a reputation as a responsible steward of information.
- We provide consumers with *notice*—the ability to know what and for what purpose personally identifiable information about them is collected and used.
- We provide consumers with *choice*—the ability to *opt-out* of our use of marketing information about themselves; and where feasible, the ability to *opt-in* to certain marketing uses.
- When feasible, we provide consumers with *access* to and a correction procedure for personally identifiable information about themselves used for non-credit-marketing purposes.
- To ensure *data integrity and security,* we employ state-of-the-art technology and tested procedures to collect, store and transmit personally identifiable information. Because commerce and our reputation are on the line, we have a vested interest in the quality of the information in our databases. Thus, we employ stringent practices and procedures to maintain the highest standards of data accuracy, reliability and completeness that humans and technology can achieve.
- Equifax provides individuals with meaningful and practicable *remedies and redress* in the event individuals are harmed by the misuse of personally identifiable information about them. These remedies arise from several sources: Equifax adherence to our own privacy principles and to other industry self-regulatory principles governing the use of personally identifiable consumer and commercial information; adherence to the requirements of the BBB Online Privacy Seal; from the Federal Trade Commission's enforcement of the unfair and deceptive practices provisions of its charter, and from compliance with US and international laws, including the European Union Data Protection Directive.

Core Value II: Equifax supports and has launched business self-regulatory and marketplace initiatives designed to balance the substantial societal benefits of the free flow of information and the legitimate concerns about the privacy of personally identifiable data.

- Equifax adheres to the privacy principles and requirements of the BBBOnline Privacy Seal, the Online Privacy Association, and the Direct Marketing Association, as well as to the information-use initiatives of the Coalition for Sensible Public Record Access (CSPRA) and the Associated Credit Bureaus, Inc.
- Equifax will only do business with entities that adhere to meaningful fair information practices that effectively address the concepts of notice, choice, access, security, and redress.
- Equifax enlightens, enables and empowers consumers to monitor their financial health using product solutions to address consumer privacy issues such as identity theft and credit score disclosure.
- Equifax employs and provides our customers with patent-pending identity authentication technology and a wide range of other products and services that enable our business customers to make sound risk assessment decisions and rel-

evant marketing offers to consumers through the appropriate and ethical use of personally identifiable information.

- Consumers and business both expect to conduct business transactions instantaneously and securely. The free flow of relevant information to legitimate businesses makes this possible.
- Legitimate business access to relevant consumer information is critical to achieving a number of societal benefits: thwarting identity theft, locating estate heirs, witnesses, child support delinquents, debtors, missing children, organ donors, etc.

Core Value III: Equifax seeks opportunities to work harmoniously with governments, consumers and businesses to forge effective solutions to the complex privacy and ethical information-use issues worldwide.

- Governments first must enforce existing laws concerning use of personally identifiable information and should consider enacting applicable laws only after industry self-regulatory measures fail.
- If industry self-regulatory initiatives fail after being given a fair chance, Equifax then supports government regulation that is relevant, not unduly restrictive, and that clearly resolves the perceived imbalance.
- In an e-commerce, online environment, national governments must adopt preemptive measures to ensure that the transmission of information and online transactions are seamless across geographical boundaries.
- In considering privacy law and policy, governments should recognize the differences between the impact of and the potential harm arising from the use of personally identifiable information for financial decisions and that used for marketing or other less serious purposes. Privacy laws should pivot not on the source, but on the content and the use of the individual information.
- Consumers must take some responsibility for educating themselves about privacy policies, procedures, products, and technologies that enhance consumer information protection and increase trust in transactions.
- Under the privacy bargain, consumers should expect the level of information privacy protection commensurate with their demands on business, the benefits sought and the sensitivity of the information exchanged.
- Businesses that collect, maintain and use personally identifiable data have a responsibility to develop and implement an effective privacy program and to employ ethical information practices.
- The business community has a responsibility to develop products and services that allow consumers to participate safely in the information marketplace and to protect their own privacy.
- Equifax has taken the lead by providing online solutions that enlighten, enable and empower consumers to manage their financial health. These easily accessible products allow consumers to examine their credit file, monitor changes in it to thwart identity theft, and to obtain and understand their current credit score.
- Equifax will continue to develop products and services and, in concert with other industry members and associations, develop programs designed to empower and enable consumers and customers to better manage privacy and risk issues.

IV. CONCLUSION

In sum, direct marketing is a societal and economic good. The process is profitable, efficient and benign. The concept is consumer oriented and privacy sensitive.

In closing, I want to thank you again for the opportunity to testify and to congratulate the Chairman and the Subcommittee for their leadership in the privacy arena. We look forward to working with you so that the marketplace might achieve the synergies that can arise from a greater understanding and appreciation of the important societal benefits of direct marketing—that is, efficient direct marketing conducted in a self-regulatory environment that embraces effective privacy protections.

Mr. STEARNS. Thank you, Mr. Ford. And we have corrected our—we have you as Chief Privacy Officer, instead of Policy Officer, and we are sorry.

Mr. FORD. Thank you.

Mr. STEARNS. Opening statement?

STATEMENT OF DEBORAH ZUCCARINI

Ms. ZUCCARINI. Good morning, Mr. Chairman and subcommittee member Towns. Thank you for the opportunity to address the subcommittee as it studies information use, particularly as it relates to marketing.

My name is Deborah Zuccarini. I am Executive Vice President and Chief Marketing Officer for Experian Marketing Solutions. My comments today summarize key issues addressed in a much more detailed statement I have submitted for the record.

Experian is one of the world's leading information services providers, with more than 30,000 North American customers. Our information solutions help businesses in over 50 countries expand their markets, make sound lending decisions, and provide the products and services their customers need and desire.

We have been responsible stewards of the information we collect, maintain, and utilize for decades. Experian takes information security and consumer privacy very seriously. Our business practices and culture reflect our resolve to ensure information is used to bring benefit to both businesses and consumers, while ensuring consumer privacy is protected. A thorough discussion of our approach to privacy is included in my written statement, including consumers' choice to opt out.

There is a great deal of misunderstanding about marketing information use, which has led to a number of popular myths about direct marketing. During the next few minutes, I would like to try to dispel a few of the most pervasive myths.

I suspect the myth most responsible for this meeting is that marketing information is used to create detailed individual consumer profiles. That simply is not true. Mr. Chairman, subcommittee member Towns, with all due respect, data compilers don't care who you are as an individual. From our information, marketers want to know about the general characteristics of their overall market or key market segments. Specific characteristics about a single individual do not provide useful marketing insight. For that reason, marketing data bases typically are not designed to provide a list of one.

Our marketing information consists of estimated or modeled data, summarized U.S. Census data, other publicly available information, or self-reported consumer survey data. It is typically used to reach lists of thousands of consumers with an offer of interest to them, not to review a single record about an individual.

In the end, direct marketing using our compiled data is just advertising. Just as television advertising brings you the Super Bowl, direct marketing advertising brings you the products, services, and other benefits that businesses have to offer. Direct marketing allows many small businesses and new market entrants to advertise and compete, even without a Super Bowl budget.

The second common myth is that marketing information is used for individual look-up. Experian marketing information services are not utilized to locate, identify, or verify the identity of individuals. In fact, our contracts prohibit the use of marketing information for such applications. In the information industry, we refer to such information use as individual reference services. We separately offer these services to law enforcement and other qualified users such as

government agencies, who use the services for child support enforcement, locating witnesses and victims, and preventing fraud. However, such services are not derived from information compiled for marketing purposes.

The third myth I would like to address today is that marketing information is used for credit, insurance, or employment underwriting. This is not the case. This myth arises from confusion between marketing information and credit reporting. The Fair Credit Reporting Act governs third-party information used for credit, employment, or insurance underwriting. Use of a marketing data base for FCRA-permissible purposes could subject that data base to all of the requirements of the FCRA, making it unusable for marketing. Therefore, Experian prohibits such use. And that is why the urban legend about grocery store purchases being shared for insurance underwriting is just that—a legend.

These and other misunderstandings contribute to heightened privacy concerns. We understand and respect these concerns, and we work diligently to ensure consumer privacy is protected. Experian believes that marketing information use is not a privacy threat, but it is vital to our economy.

In the privacy debate, there seems to be an assumption that such information use somehow causes harm, yet no evidence of real harm has been shown. Hard questions must be asked to determine if any real or perceived harm truly outweighs the demonstrated economic benefits of information use for marketing. A recent study by the Information Services Executive Council estimated consumers save over $1 billion annually as a result of information sharing in the catalogue apparel industry alone. A WEFA Group study estimated that in the year 2000, total consumer sales attributable to direct marketing would be nearly $940 billion, and that more than 14.7 million people would be employed throughout the U.S. economy as a result of direct marketing activities.

We believe that responsible information use for marketing is in the best interests of both businesses and consumers. The quality of offers today has improved significantly over the years, resulting in greater efficiency for businesses, lower costs for consumers, less mail, and more opportunity.

Mr. Chairman, this concludes my remarks. Thank you for inviting Experian to present our view on these important issues. We would be happy to answer any questions you or other subcommittee members may have.

[The prepared statement of Deborah Zuccarini follows:]

PREPARED STATEMENT OF DEBORAH ZUCCARINI, EXECUTIVE VICE PRESIDENT AND CHIEF MARKETING OFFICER, EXPERIAN MARKETING SOLUTIONS

SUMMARY

For more than 50 years Experian has been a leader in the information industry. In fact, the company's roots date back more than 100 years to the pioneers of credit reporting. Its success is based on sound information values that guide the development of practices and policies that protect consumer privacy, ensure security and provide benefit to consumers and our business clients alike.

Responsible information use today affords consumers greater choice, convenience, and lower prices than ever before. In past decades, our economy was local. Consumers lived where businesses were located. Product and service choices were limited to what was available in a consumer's neighborhood, the local main street, or

perhaps a nearby city. Consumers learned about businesses by walking down the street, or reading ads in the local newspaper.

Today, our economy is national. Businesses in Los Angeles and New York compete daily for sales to consumers in Kansas. Where once there was only a single provider of a product or service, or maybe two or three to choose from, there now are hundreds. Because of responsible information sharing, those businesses can reach consumers who are most likely to need their products and services. That greatly increases consumer choice and promotes competition, which drives down prices.

Unfortunately, a number of myths and misunderstandings have arisen about information use for marketing purposes. Those myths and misperceptions are the basis for many of the privacy concerns that have brought us here today. This testimony attempts to dispel three of those myths:

- **MYTH: Marketers want to know specific information about individual consumers.** In fact, marketers don't focus on individual consumers. Instead, they are interested in overall market characteristics.
- **MYTH: Marketing databases are used for individual "look-up."** In reality, marketing information is used for overall market analysis. It is not used to identify, locate, or verify the identity of individuals.
- **MYTH: Marketing information is used for credit, insurance or employment underwriting.** The Fair Credit Reporting Act governs information use for these purposes. Therefore, marketing information is not utilized for these purposes.

Unintended and unforeseeable consequences of new legislative mandates based on such myths may jeopardize today's robust, information-based economy.

Dozens of federal and state laws govern information use for marketing purposes, along with multiple industry self-regulatory regimes. We are concerned that current legislation may already have gone too far, and has failed to balance economic vitality with legitimate consumer interests.

Legislation already strictly controls the use of sensitive information, including credit, financial, medical and children's data. Additional government-mandated restrictions on marketing information use may result in unexpected and unintended consequences. Small businesses, relying on cost-effective direct marketing as an advertising channel, could be forced out of the marketplace, diminishing consumer choice and opportunity. Yet, consumers would likely not benefit from any substantive privacy protections.

Experian applies stringent information values to all of its information uses through a strict assessment process that ensures privacy concerns are addressed and that the information use benefits both businesses and consumers.

We consider ourselves to be stewards of the information we collect, maintain and utilize. Our responsibility is to ensure the security of the information in our care is protected and that the privacy of consumers is maintained through appropriate, responsible use.

Through its Consumer Advisory Council, Experian receives valuable insight and guidance from consumer advocates, legislators, scholars and business leaders regarding our information services. In addition, our Corporate Privacy Council, a group of company leaders, meets regularly to ensure Experian information services provide consumer and business benefit while upholding the Experian Information Values and ensuring privacy expectations are met.

Although the pervasive myths discussed above inaccurately suggest otherwise, Experian and others in the direct marketing industry work diligently to understand and address consumer privacy concerns. We encourage you to continue to study the importance of information flows to our economy. We believe the current legal and self-regulatory framework best serves consumers and businesses. The greatest consumer and business benefit is achieved through consumer notice and the opportunity to opt-out.

ABOUT EXPERIAN

Experian is one of the world's leading information solutions companies. Primarily involved in credit reporting and direct marketing services, we also provide references services, analytic services, and consulting solutions, helping businesses make better, faster decisions, and efficiently reach consumers with new product and service offerings. Our annual sales are in excess of $1.5 billion. The chart in **Appendix A** outlines Experian's history.

Experian employs more than 6,500 people in North America. Our corporate headquarters are in Orange, CA, where we have 1,364 employees. Other major U.S. employment centers include:

- Colorado—209 employees (Denver)

- Georgia—157 employees (Atlanta)
- Iowa—585 employees (Mt. Pleasant)
- Illinois—1,398 employees (Lombard, Schaumburg)
- Nebraska—1,218 employees (Lincoln, Seward)
- New Jersey—79 employees (Parsippany)
- New York—220 employees (Albany, New York, Rye)
- Texas—802 employees (Allen, McKinney)
- Vermont—263 employees (Rutland)

EXPERIAN'S PRIMARY BUSINESS AREAS

Experian has six key business areas: direct marketing services, credit reporting, automotive information services, customer relationship management, electronic commerce services and individual reference services.

Direct marketing services

Experian direct marketing services help bring businesses and their customers together. The company touches nearly one in four pieces of mail delivered by the U.S. Postal Service. But Experian direct marketing services extend beyond targeted mailing. Businesses rely on Experian to help them better understand their markets and the characteristics of the people who do business with them. Understanding the marketplace makes possible faster, more efficient product development and delivery, better retail outlet and service center locations, improved customer service, more cost-effective advertising and lower costs for consumers.

Each year, Experian ships 1.7 billion pieces of mail from its processing centers and provides address information for more than 20 billion promotional mail pieces delivered to more than 100 million households. Those offers present consumers with products and services from companies about which they may otherwise never have known. By identifying the characteristics of consumers likely to be interested in certain kinds of products and services, Experian helps marketers more efficiently reach consumers who are most likely to be interested in a business' products or services.

Credit reporting

Experian and the companies from which it was formed have provided credit reporting services for more than 100 years. J.E.R. Chilton began credit reporting in Dallas, TX in 1897 by taking notes from local merchants in a little red book. Decades later, the TRW Corporation pioneered computerization of the credit reporting process, leading to a national credit reporting system. In 1996, TRW sold its credit reporting unit, which became Experian.

Today, hundreds of millions of credit reports are provided to lenders annually. The ability of creditors to check a person's credit references in an instant enables them to make rapid, sound, and objective lending decisions. That ability helps consumers get the credit they need and deserve faster and cheaper than anywhere else in the world. Enabling lenders to make objective, safe, secure loans and minimize other credit-related losses, while providing consumers instant access to credit, has contributed greatly to the robust U.S. economy.

Customer relationship management

Business success is built upon positive relationships with customers. Relationships are built on information. Experian helps businesses establish and develop long-lasting customer relationships through responsible information use. We help businesses get a clearer picture of their customers across multiple business units and market segments. We help companies understand why certain kinds of people shop with them and what the customer needs. With that clearer understanding, Experian then is able to provide information services that help businesses initiate relationships with new customers, assist the businesses in developing new, desirable products and services and aid in providing pleasant shopping and effective customer service. The result is a better shopping experience for consumers and more profitable operation for businesses.

Automotive Information Services

Experian Automotive Information Services specialize in the collection and dissemination of vehicular data from each of the 51 United States jurisdictions. The information is utilized to provide valuable services to auto dealers, manufacturers, consumers and advocacy organizations, advertising agencies and internet information sites, law enforcement and tollway authorities. Detailed vehicle history reports enable consumers to make informed used-auto purchasing decisions. Manufacturers rely on our services to manage recalls and conduct market analysis to manage product supply and improve service.

Electronic commerce services

Experian's electronic commerce division helps businesses establish a presence in the electronic marketplace, develop relationships with online consumers and ensure consumers and businesses enjoy positive, safe transactions. Our e-commerce division focuses on both consumers and the businesses that reach them with patented delivery systems and best-in-the-industry security processes and systems.

For our business partners, we verify, authenticate and enhance identity information about consumers and businesses. With enhanced authentication, clients reduce fraud by making confident transaction decisions in real time.

For consumers, we offer a range of personal information solutions ranging from our online credit report with real-time dispute registration, to our vehicle history report—a must for used car purchases. We offer a subscription service for unlimited access to credit report and credit score information along with the tools required to better understand them. We also offer a property report—to better understand the value of your home—or prospective home.

Individual reference services

Our reference services help people, businesses, non-profit organizations, government agencies, law enforcement, and other organizations identify, locate, and verify the identity of individuals. The most recognized individual reference services are the telephone book and directory assistance—services you use every day. They usually include only names, addresses and telephone numbers.

More sophisticated reference services may include information about whether you own a home or rent an apartment, how long you have lived in the same location, and if there are additional household members.

Sensitive identifying information such as your Social Security number, driver's license number, and date of birth is included in some reference services. These services, however, are limited to use by law enforcement, government agencies, and other organizations with a legitimate and appropriate need for such information.

THE BENEFITS OF INFORMATION USE

Because of the information services provided by Experian and its counterparts, the United States has the most robust economy in the world, and its consumers have greater choice and receive greater value than consumers anywhere else in the world.

Consumer benefits of information use

Direct marketing: Direct marketing services increase choice and opportunity and reduce costs. Each year, Experian ships 1.7 billion pieces of mail from its processing centers and provides address information for more than 20 billion promotional mail pieces delivered to more than 100 million households. Those offers present consumers with products and services from companies about which they may otherwise never have known. By identifying the characteristics of consumers likely to be interested in certain kinds of products and services, Experian helps marketers reduce unwanted mail and send only offers that consumers are likely to want or need. But targeted mail processing is only one of many direct marketing services provided by Experian and its industry associates.

Market analysis services help businesses identify the common characteristics of their customers. A richer understanding of their customer base helps businesses better plan media campaigns, determine retail site location, develop new product offerings, better position their brands, have a clearer understanding of their customers' service needs, and reach new customers. For consumers, the result is lower product cost, better customer service, more convenient shopping, faster delivery, reduced unwanted mail and exposure to useful new products and services.

An April 2001 study by the Information Services Executive Council found restrictions on marketing information use would cost catalog and Internet apparel shoppers $1 billion annually.[1] According to the study, that cost would be shared disproportionately by inner city and rural catalog shoppers. Inner city neighborhoods generally are under-served by traditional retail stores, and rural consumers often live long distances from the nearest mall or retail center. As a result, these two groups are more reliant on catalog or Internet shopping alternatives.

Similarly, a December 2000 study by Ernst & Young found members of the Financial Services Roundtable (FSR)—a group of 90 of the nation's top banking, insurance and securities firms—save approximately $1 billion a year by using targeted marketing. Much of that savings is passed directly on to consumers.[2]

"FSR members report that they would send out about three to six times more direct marketing if they could not use information sharing for targeted marketing.

Targeted marketing results in real savings for financial institutions, some or all of which will be passed forward to customers in price reductions," the study said.

According to the study, FSR customer households annually save $17 billion and 320 million hours as the result of information sharing among affiliates and third parties.

Credit reporting: The United States' unique credit reporting system dramatically increases American consumers' choices and opportunities for financial services. Because of the U.S. automated credit reporting system, American consumers can obtain credit and secure other financial services at lower costs from a larger number of providers than anywhere else in the world.

By comparison, economist Walter Kitchenman said of nations without an open credit reporting system, "As a result, financial services are provided by far fewer institutions—one-tenth the number serving U.S. customers, despite the fact that the pan-European market has almost one and one-half times as many households."[3] He added, "consumer lending is not common, and where it exists, it is concentrated among a few major banks in each country, each of which has its own large databases. "In fact, European consumers, although they outnumber their U.S. counterparts, have access to *one-third* less credit as a percentage of gross domestic product."

The open U.S. credit reporting system provides a foundation for lender confidence, increasing the availability of loans, reducing the cost of credit and increasing competition for customers, all of which benefit the U.S. consumer.

Individual reference services: Often the benefits of individual reference services, and the services themselves are taken for granted. Yet they are used everyday. People, businesses, law enforcement and other organizations utilize individual reference services routinely to locate, identify and contact people for a variety of very positive reasons. Basic reference services, such as a telephone book, are available to almost anyone. Experian separately provides more sophisticated services only to law enforcement or other qualified users. A few of the users of individual reference services and how such services are utilized are listed below.

- **You:** through the telephone book or directory assistance to find a telephone number or an address to send a thank you note or holiday greeting.
- **Lenders, retailers, e-tailers:** to verify the identities of potential customers and protect you from fraud.
- **Law enforcement agencies:** to locate crime witnesses and apprehend criminal suspects.
- **Child support agencies:** to locate parents who are behind in their child support payments.
- **Government agencies:** to find missing pension fund beneficiaries and heirs.
- **Alumni Associations:** to contact recent graduates and send event notices to current members.
- **Businesses:** for product recalls and product notices.

The information included in individual reference services can range from just names, addresses and telephone numbers, to more sensitive identifying information including dates of birth, Social Security numbers and drivers license numbers. Access to certain types of reference information is carefully monitored and controlled. For instance, an individual only is allowed access to published telephone book information. Law enforcement agencies, however, can access more sensitive data for use in criminal investigations.

During 1998, the FBI made 53,000 inquiries into commercial individual reference services. According to then FBI Director Louis Freeh, utilization of these services aided in the arrest of 393 fugitives, identification of more than $37 million in seizable assets, locating 1,966 wanted individuals and location of 3,209 witnesses wanted for questioning.[4]

Overall economic benefits of information use

Experian information services promote competition in the marketplace. Information sharing for target marketing and credit reporting opens the door for small, emerging businesses to compete with larger, established companies. It levels the playing field by making the cost of entry affordable to everyone.

Information sharing "allows new market entrants, which cannot afford mass market advertising and lack the customer lists of their well-established competitors, the ability to reach those people most likely to be interested," said Fred H. Cate and Michael E. Staten in their paper, *Putting People First: Consumer Benefits of Information-Sharing.*[5]

According to the Ernst & Young study, "FSR members save about $1 billion per year through targeted marketing based on shared information—savings that can then be passed forward to customers. Almost all of the survey respondents said that

if they could not use targeted marketing, they would resort to mass marketing instead, while a few said that they may eliminate direct marketing completely."[6]

The implication is that large companies could bear the cost of mass marketing—ostensibly unfettered distribution to every U.S. consumer. For small businesses, it means being forced out of the marketplace. With reduced competition, consumers would be faced with higher prices and less choice. The French financial banking industry provides a good example.

In a 1999 study, Walter Kitchenman said:

> In France, for example, the EU country with the strictest financial privacy laws, seven banks control more than 96 percent of banking assets. The seven dominant French banks, each with assets of over $100 billion, already own extensive databases—and don't need to share customer information with anyone. The fact that this system restrains innovation, hurts customer choice, and increases price is not a great concern to those banks because the same system also restrains competition and makes it easier to hold customers and capital captive.[7]

As he points out, while solicitations may sometimes seem annoying to consumers, the solicitations in fact represent a free flow of information that promotes competition among businesses of all sizes, giving U.S. consumers far more choice and opportunity at significantly lower costs.

The direct marketing industry also is an important source of employment and a significant part of the overall consumer market. A recent WEFA Group study estimated that in the year 2000, total consumer sales attributable to direct marketing would be nearly $940 billion. The same study estimated more than 14.7 million people would be employed throughout the U.S. economy as a result of direct marketing activities.[8]

Building relationships between businesses and consumers

It has been said that credit reporting is a secret ingredient of the U.S. economy's resilience. The availability of automated, nationwide credit histories enable lenders to make objective, sound lending decisions, reducing risk, attracting investment and strengthening the economy.[9] As a result, U.S. consumers benefit from widely available credit at lower costs than anywhere else in the world. Some estimate that because of the U.S. credit reporting system, consumers in this country save as much as $80 billion a year on mortgage loans alone.[10] But the robust nature of the U.S. economy does not rest only with information use for credit reporting purposes.

Direct, or target, marketing results in significant savings for businesses each year. Those savings are passed on to consumers. An Ernst & Young study indicated members of The Financial Services Roundtable (FSR) would have to send out three to six times more marketing offers if they could not use information sharing for targeted marketing purposes. The result would be far greater costs, which would be passed on to consumers, not to mention increased volumes of mail in their mailboxes.[11]

Restricting information use also threatens the backbone of the U.S. economy: small businesses. Today, small businesses rely on the availability of information to establish and expand their markets. They could not compete with corporate giants if they were unable to utilize target marketing to reach consumers who otherwise would not even know the business existed. Experian provides marketing solutions to almost 4,000 small businesses across the country.

In a July 2000 paper, Fred Cate and Michael Staten presented very clearly the danger to our economy of interfering with information sharing:

> Interfering with the availability of that information hurts both consumers, who miss out on opportunities, and businesses, who face higher costs to reach consumers, but such interference imposes an especially heavy burden on small companies, which cannot afford mass market advertising and lack the customer lists of their well-established competitors. Open access to third-party information and the responsible use of that information for target marketing is essential to leveling the playing field for new market entrants.[12]

The ISEC study reached the same conclusion when looking at an opt-in approach to marketing information as opposed to the current opt-out standard. Implementation of data use restrictions would drive up total costs to consumers from 3.5 to 11 percent. The result would be devastating to small firms and new market entrants.

According to the study, "Since marketing costs will likely increase if external opt-in restrictions are put in place, some retailers will be forced to exit the market and other, new companies will be deterred form entry. With a smaller marketplace, competition suffers, giving consumers less choice and higher costs when distance shopping."[13]

It is easy to overlook the impact of information use on our local, small businesses. We too often take for granted the local food store, pharmacy or men's clothing store. In today's economy, they are competing not only with giant supermarkets, drug outlet stores and shopping malls, but also with online services that may deliver to your door. In such an environment, information sharing is critical for small businesses just to maintain a storefront in the community.

Detecting and preventing fraud

Experian's information services are a key resource in providing assistance to businesses, consumers and law enforcement to detect, stop and recover from fraud—both online and offline. Consumer information maintained under Experian's stewardship is fueling new, state-of-the-art online verification and authentication systems, including digital signatures. The new technology, used responsibly, is critical to the continuing growth of e-commerce.

Individual reference services provided by Experian help law enforcement identify and locate suspects and perpetrators of fraud, speeding arrest and prosecution.

Recently, Experian launched the National Fraud Database, the nation's first repository of known fraudulent activity. Participants include representatives from a variety of industries, such as financial services, insurance, retailing and telecommunications. Members contribute known fraud data to Experian, which then enters it into the database. A National Fraud Database Report will be provided to a participating lender, for example, when a loan application is submitted. Information in the report matching a previously verified fraud case will help lenders prevent fraud from occurring at the point of origin.

Participation in this ground breaking initiative has been offered to Experian's competitors—Trans Union and Equifax—as a way of solidifying the industry's resolve to fight fraud and identity theft.

HELPING BUSINESSES BUILD CUSTOMER RELATIONSHIPS

Why marketing information is important to businesses

Businesses rely on Experian to provide accurate, reliable information services that help them better understand their markets and identify, contact and build profitable relationships with new customers. Experian's information solutions help businesses better understand their markets and more efficiently reach consumers likely to be interested in the products and services the businesses offer. That reduces marketing costs and increases new customer satisfaction. Customer analysis and resultant market segmentation also enables business to tailor their advertising outlets to reach interested consumers, better position their brands, improve customer service, and better locate retail outlets and delivery centers. The result is greater efficiency, lower costs passed on to consumers, greater customer satisfaction and increased customer loyalty, all of which make a business more successful.

Some myths about marketing information use

There are a number of myths and misperceptions about direct marketing and the information in direct marketing databases. Many of these myths appear to drive the debate about increasing restrictions on marketing information to protect consumer privacy. Here are a few of those myths and the facts that will help dispel them.

1. MYTH: Marketers want to know specific information about individual consumers. Direct marketing is simply another form of advertising, not unlike television ads aired during the Super Bowl. Like Super Bowl advertisers, direct marketing advertising are attempting to reach a large group of individuals who have certain demographic characteristics that indicate they may be interested in purchasing their products or services. Unlike Super Bowl advertisers that have millions of dollars to spend on promotions, direct marketers often are small businesses, or new market entrants without large budgets. Therefore, they need more efficient ways to advertise to their marketplace.

Marketing databases are not designed to provide a "list-of-one." Instead, businesses want to know about the characteristics of their overall market. The consumer characteristics of a single individual do not provide useful market insight. Once a market is better understood, a business may want to send an offer (whether offline or online) to hundreds, thousands, or even tens-of-thousands of consumers. For that they may receive a mailing list of names and addresses, but again, the business is not interested in the specific information about a single individual.

Further, information in most marketing databases is summarized at the household, not individual level. Rather than analyzing information about specific individuals, businesses typically consider household-level information. Much of that information is estimated or modeled using U.S. Census data or consumer survey data. Estimated age and income ranges and general interests are examples. For more in-

formation about the types of information utilized for direct marketing and information sources, see **Appendix B.**

2. MYTH: Marketing databases are used for individual "look-up." Experian marketing information services are not utilized to locate, identify or verify the identity of individuals. Our contracts prohibit the use of marketing information for such applications.

In the information industry, we refer to such information use as individual reference services. Appropriate use of these services is ensured through a strict self-regulatory code and related industry practices.

Although you don't realize it, you probably use reference services every day. The most common is the telephone book.

Experian separately offers more sophisticated services to law enforcement and other qualified users, such as government agencies, who use the services for child support enforcement, locating witnesses and victims, and preventing fraud.

However, such services are not derived from information compiled for marketing purposes.

Marketing databases are used for overall market analysis and identifying households with consumers who are most likely interested in purchasing a product or service. The information in marketing databases generally are not intended to be used to locate, identify or verify the identity of individuals and is not used in that manner. Again, marketing databases are not designed to return a "list-of-one."

3. MYTH: Marketing information is used for credit, insurance or employment underwriting. The Fair Credit Reporting Act governs third-party information used for credit, employment or insurance underwriting. Use of a marketing database for FCRA permissible purposes would subject the database to *all* of the requirements of the FCRA. The database then could be used only for FCRA permissible purposes. It could no longer be used for marketing.

For that reason, Experian's marketing database and credit reporting database structures are entirely different and distinct.

And it's why the legend about grocery store purchases being shared for insurance underwriting is just that—a legend.

COMPILING AND UTILIZING INFORMATION FOR MARKETING PURPOSES

Experian is a data aggregator. Our company collects and maintains information for marketing purposes and provides information solutions enabling marketers to efficiently reach consumers who are interested in purchasing their products and services. We are committed to providing information solutions that benefit both our business clients and consumers. We also recognize and take very seriously our responsibility to protect consumer privacy.

We must ensure the security of the information we collect and maintain, and ensure that it is used appropriately. Experian takes a "values approach" to privacy, which is described in greater detail below.

We provide consumers with notice regarding our information collection and use and choice regarding that information collection and use including an opportunity to opt-out of information collection and use by Experian.

To opt-out of Experian marketing information use, consumers need only call 1 800 407 1088.

Experian also is a member of the Direct Marketing Association (DMA). We honor the DMA mailing and telephone preference lists.

The following sections describe Experian's role as a data compiler and our approach to addressing privacy issues.

Experian's role as a data compiler

Experian marketing databases contain information about more than 98 percent of U.S. households. The information is utilized to help businesses analyze their overall markets and market segments and to contact consumers who will most likely be interested in the products and services they offer.

Experian maintains databases for two distinct purposes: credit reporting and direct marketing. The data for those uses is kept separate, both physically and electronically. Experian's credit reporting database is physically located near Dallas, TX. Its marketing databases are in Schaumburg, IL. The information is maintained and utilized for appropriate purposes and is not combined or commingled except as allowed by law.

The information Experian collects

The information Experian collects for direct marketing purposes comes from a number of sources, first and foremost directly from consumers. Warranty cards, surveys, magazine subscriptions and sweepstakes entries all are provided by consumers

and are utilized for direct marketing services. Other sources include non-personally identifiable United States Census information, public records and telephone directory information. Experian direct marketing information includes:

- Census information (median or percentage values based on census track)
- Lifestyle information (reported by consumers)
- Interests, hobbies, activities
- Public records/telephone directory information

For more information about the types of information utilized for direct marketing and information sources, see **Appendix B.**

Ensuring appropriate information use

Experian found that rigid rules directing information use are quickly outdated by today's rapidly evolving technology and constantly changing consumer and business needs and expectations. For more than a decade Experian has taken a values approach to information use. Our five global information values ensure Experian information services provide value and benefit to both businesses and consumers while still enabling adaptation to cultural and regulatory changes and technological advances.

The Experian global information values are:

Balance

Experian strives to balance the interests of consumers with the business needs of customers to ensure both receive benefit from information use.

Accuracy

Experian strives to ensure the information it collects and maintains is as accurate and up-to-date as possible and that the information is appropriate for its intended use.

Security

Experian protects the information it maintains from unauthorized access or alteration.

Integrity

Experian complies with all laws and applicable industry codes and operates its businesses in accordance with these information values.

Communication

Experian communicates openly about the information it maintains, how it is used and seeks to inform consumers of their rights regarding the use of information.

Every Experian information service undergoes a formal Information Values Assessment before it is approved. The assessment ensures the service not only meets all legal and self-regulatory requirements, but that it also meets security standards, addresses consumer privacy concerns and provides value and benefit to both businesses and consumers.

Teams within each Experian business unit is tasked with ensuring new information services undergo values assessments. These individuals and their teams work integrally with Experian sales staff and marketing units to ensure the Information Values are built into all of Experian's products and services.

In addition, Experian seeks input from consumer groups, consumer advocates and its business partners regarding information use to further ensure the services it provides incorporate appropriate security and privacy provisions and provide benefit to both consumers and its business clients.

Our Consumer Advisory Council was among the first organizations of its kind. Composed of consumer advocates, legislators, scholars and business leaders, the Council provides valuable insight and guidance regarding Experian information services. Consumer Advisory Council opinions and suggestions help us provide information services that provide value and benefit to both businesses and consumers while effectively addressing privacy issues.

The Experian Corporate Privacy Council is comprised of senior-level managers. Its members meet regularly to discuss and address privacy issues and to ensure Experian information services uphold the Experian information values and exceed privacy expectations.

Experian is committed to providing consumers with notice and choice regarding its information services. Whenever Experian direct marketing services are utilized, consumers must be given notice of the information use and provided with an opportunity to opt-out of that information use. To opt-out of Experian marketing information use, consumers need only call 1 800 407 1088. We comply strictly with the Di-

rect Marketing Association (DMA) Privacy Promise and honor the DMA opt-out lists.

Consumer education

We produce a number of education materials that describe how information is collected and utilized, our Information Values and information use policies and consumer choices regarding information collection and use. All of the materials are provided free to consumers through many partnerships, among them:

- State attorneys general
- State and federal legislators' offices
- State and federal government agencies
- The United States Army
- The United States Navy
- Offices of consumer affairs
- Consumer organizations
- High school and university educators
- Student organizations
- Divorce attorneys
- Marriage counselors
- Realtors
- Lenders
- The media

There are many others. Experian is committed to reaching consumers with the information they need to understand how they can be actively involved in our information economy.

We have delivered to consumers more than 1 million copies of our various *Reports on* series. Our four-part *Reports on Direct Marketing* describe how the direct marketing process works, what information Experian collects and how it is used, and provides details on the choices consumers have and what they need to do if they choose to opt-out.

Hundreds-of-thousands of Experian's *booklet 12 Common Questions about Credit Reporting and Direct Marketing* have been distributed directly to consumers and through our many partnerships. The booklet is printed in both English and Spanish versions.

Much of the consumer education material is available online. Experian also offered the first online advice column about information use, called *Ask Max.* During the past four years, more than 50,000 questions have been received from consumers, and more than 100 columns have been published. Most column responses address credit reporting issues because few consumers have submitted questions about direct marketing.

Access

Marketing databases often are erroneously compared to credit reporting databases. However, the data, data uses and structures of marketing databases and those of credit reporting databases are entirely different. Comparison is, to use a cliché, apples and oranges. To suggest an access and dispute process for marketing databases like that for credit reporting is unrealistic.

The information in a credit reporting database is used to make critical lending, insurance, housing and employment decisions about specific individuals. Therefore, the data must be as precise as possible. Because the information is specific to the individual and of such a crucial nature, consumers need to know and have the ability to play a role in ensuring the accuracy of the information. Information service providers store data and manage its use. The source of the information generally must correct any inaccuracies and update that information with the credit reporting agency, which essentially serves as a library.

Marketing databases also serve, in a sense, as a library. But the nature of marketing databases makes such a disclosure and dispute process very impractical, if not impossible.

Unlike lenders, who need to know precise details about an individual's repayment history, marketers need only to understand the general characteristics of their overall markets. By identifying those characteristics, businesses are better able to reach consumers who will most likely be interested in purchasing the products and services they offer. Because marketers need only to contact a broad group of consumers who may be interested in a product or service, the information in marketing databases is not precise. In fact much of the information in marketing databases is derived from computer models, is estimated or is presented in ranges.

Consumers would expect a level of precision and accuracy that simply is not present, which would make a dispute process impractical, if not impossible. Because

most information in a marketing database is of this nature, such a disclosure would be of little, if any benefit to the consumer.

While providing a disclosure would be of little benefit, it likely would pose a greater threat to privacy than currently exists. The nature of marketing databases would limit identification authentication largely to name and address, which is widely available in public sources, such as telephone directories. Access requirements, therefore, should be constructed by balancing the benefits to consumers against the risks to them and the costs to companies that hold the data.

Requiring access would require information aggregators like Experian to create the very kind of database you are most concerned about. In order to provide access, a marketing database would have to include detailed, personal information that could be compiled and provided easily and quickly in highly detailed individual dossiers. This is the very thing we want to avoid.

Allowing access to marketing databases would be enormously expensive. In fact, it would require retooling of an entire industry. Existing database architecture would have to be redesigned and disparate databases linked together to form name-driven profiles. Large customer service staffs would have to be hired and stringent security safeguards put in place. While that expense is justified and necessary with regard to information governed by the Fair Credit Reporting Act, it is of questionable value for data collected only for marketing purposes.

A consumer's current ability to opt-out of having their name shared for direct marketing purposes satisfies the underlying concern about privacy without imposing undue and unnecessary costs to businesses and risks to consumers that would result from access requirements.

The current regulatory environment

A significant body of legislation and self-regulatory regimes already govern the use of consumer information. All information collected and utilized by Experian is governed either by specific legislation or industry self-regulatory guidelines. The following lists describe the statutory and self-regulatory regimes currently governing information use for marketing and credit reporting purposes, for both online and offline applications.

Regulatory requirements governing marketing information:

- Drivers Privacy Protection Act (DPPA)
- Fair Credit Reporting Act (FCRA; for pre-approved credit offers)
- Children's Online Privacy Protection Act (COPPA)
- Telephone Consumer Protection Act and Telemarketing Sales Rule
- State do-not-call requirements
- Census Confidentiality Act
- State Voter Records Acts
- Gramm-Leach-Bliley Act

Self-regulatory standards for marketing information:

- Direct Marketing Association (DMA) Privacy Promise
- DMA Telephone Preference Service
- DMA Mail Preference Service
- DMA Electronic Mail Preference Service
- DMA Ethical Guidelines
- Experian Information Values and associated practices

Regulatory requirements for credit information:

- FCRA
- Equal Credit Opportunity Act (ECOA; relates to risk score development)
- Fair Debt Collection Practices Act (FDCPA)
- Gramm-Leach-Bliley Act

Experian supports the House Commerce Subcommittee's efforts to thoroughly investigate the issue of consumer privacy before concluding that more legislation is necessary. The Subcommittee is wise to focus on what gaps exist, if any, and whether there is a need for new regulatory mandates or enforcement regimes.

The combination of existing statutory requirements and self-regulatory guidelines of marketing information already is substantial. Experian is constantly working with its trade groups to strengthen and improve existing self-regulatory standards. For these reasons, Experian opposes further federal regulation of marketing and reference service information at this time.

The debate about privacy is incomplete and evolving. We do not yet fully understand the importance of information flows to our robust economy. Enacting legislation based on incomplete knowledge could result in additional, negative, unintended consequences to our economy and greater consumer inconvenience with no meaningful privacy protection.

The above listed regulations and self-regulatory regimes must be allowed time to work and the impact of their restrictions on information use studied. The affects of the safeguards implemented by these laws and of the recently enacted Gramm-Leach-Bliley Act are as yet unknown. It is essential that we allow some time for these new laws to bear out any unforeseen or unintended consequences.

To reiterate, Experian strongly believes existing law, industry self-regulation and market responses are providing more than adequate consumer protection.

In fact, we are concerned that current legislation may already have gone too far, and has failed to balance economic vitality against legitimate consumer interests.

The scale is often tilted by the assumption that direct marketing somehow causes harm. A number of studies, including a report by the Federal Trade Commission,[14] have found no evidence of real harm resulting from marketing information use.

Hard questions should be asked of those who claim consumers have suffered real harm. How do they define harm? Where are the examples of real harm? Is there truly harm, or are they erroneously equating harm with annoyance?

New legislation should be considered only if specific consumer harm can be demonstrated and must be implemented only in a manner that carefully balances intended consumer privacy protection against the economic benefit of accessible marketing information.

CONCLUSION

Thank you for the opportunity to submit these remarks on behalf of Experian. I hope this document helps dispel a few of the myths about marketing information use, addresses important privacy concerns and clarifies the importance of information use to our robust economy. I look forward to future opportunities to work with the subcommittee as it studies privacy and information use.

Appendix A—Experian History

Year	Event
1932	Michigan Merchants Co., later known as Credit Data Corp., is formed to provide credit-reporting services.
1966	Metromedia acquires lettershop capabilities and begins operation of its direct marketing division called Metromail.
1969	Conglomerate TRW buys Credit Data Corp.
1979	Metromedia buys Marketing Electronic Corp. to provide list enhancement services within Metromail.
1981	Direct Marketing Technology, Inc. is founded in the Chicago area.
1987	TRW buys Executive Service Co. to expand into the direct marketing industry.
	Metromail is acquired by R.R. Donnelly & Sons Co., the world's largest printer.
1989	TRW buys Chilton Corp., a credit-reporting company founded in 1897.
1996	TRW sells Information Systems & Services unit to a group of investors.
	Experian name and logo are introduced.
	Group of investors sells Experian to The Great Universal Stores P.L.C., a British conglomerate.
1997	CCN/MDS is integrated with Experian North America.
	Experian buys Direct Tech, a leading provider of list processing, database marketing, and consulting, analytical and information services.
	Direct Tech buys Brigar Computer Services.
	Metromail buys Saxe Inc., Marketing Information Technologies, and Atlantes Corp.
1998	Experian buys Metromail, a leading provider of database marketing, direct marketing, mail processing and distribution, and reference products and services.
2001	Experian buys Exactis, the global leader in multi-platform interactive marketing.

Appendix B – Elements of Experian's marketing database

Public records/telephone directory information

- Government records
- White page telephone listings
- Listed but not-yet-printed directory assistance information

Telephone directory listings
Listed white page telephone numbers
Listed but not-yet-published telephone numbers
Names
Addresses

Real estate information
(Tax assessor/deeds)
Home ownership
Property characteristics

Voter records
Name
Address
Date of birth

Occupational licenses
(State professional license records)
Medical doctor licenses
Attorney licenses
Cosmetologist licenses
(etc.)

Recreational licenses
(Fish and game records)
Hunting licenses
Fishing licenses

Appendix B – Elements of Experian's marketing database (continued)

Lifestyle information

- Activities and interests
- Consumer supplied

The most common attributes
Age
Marital status
Gender
Presence of children
Home ownership
Estimated household income

Home life
Flower gardening
Vegetable gardening
Grandchildren
Home workshop/do-it-yourself
Home video recording
Shop via TV
Surf the Internet

Good life
Attending cultural/arts events
Cruise ship vacations
Fashion clothing
Fine art/antiques
Foreign travel
Gourmet cooking/fine foods
Travel in the USA
Wines
Frequent flyer

Sports, fitness and health
Bicycling
Dieting/weight control
Golf
Health/natural foods
Physical fitness/exercise
Running/jogging
Snow skiing
Horseback riding
Walking for health
Tennis

Music
Classical
Gospel
Jazz
R&B
Rock (hard/soft)
Country
Easy listening/light sounds
Contemporary Christian
Rap

Investing & Money
Entering sweepstakes
Casino gambling
Moneymaking opportunities
Real estate investments
Stocks/bonds/mutual funds

Hobbies and interests
Automotive work
Avid book reading
Bible/devotional reading
Buy pre-recorded videos
Crafts
Electronics
Recorded music/books/programs
Needlework/sewing
Our nation's heritage
Photography
Science fiction
Science/new technology
Self-improvement
Watching sports

World and environment
Wildlife/environmental issues
Donate to charitable causes

Great outdoors
Camping/hiking
Fishing
Hunting/shooting
Powerboating
Recreational vehicles
Sailing

Appendix B – Elements of Experian's marketing database (continued)

Census information

- From United States Census reports
- Demographic information
- Aggregated, not individual data
- Based on self-reported information

Income
Median household income
Median family income
Average household income
% of households within specified income ranges

Household type
% of households with children
% of households with families
% of married couple families
% of single-parent households
% of male householder with children
% of female householder with children
% single male households
% single female households

Education
Median years of school completed by persons 25 or older
% of adults who are college graduates
% of adults with some college
% of adults who are high school graduates
% of adults with only elementary education

Home value
Median home value
Average home value
% with home values in various ranges

Age
Median age of population
Median age of adults 18 & older
Median age of adults 25 & older
% of population under age 18
% of children within various age groups
% of adults within various age groups

Occupation
% professional
% technical
% managerial
% sales
% clerical
% white collar
% craftsmen
% blue shirt
% farmers
% laborers

Other category examples:

Housing
(information about ownership, type, size, age, amenities, of housing units in a given area)
Household size
(% of households of a given size in a specific census area)
Mobility
(% of people who have moved in a given time frame)
Rent
(Median and average rent cost, % of renters paying amounts within given ranges)
Marital status
(% married, separated or divorced, widowed, or never married)
Employment industry
(% employed by certain business types)

Notes

[1] Michael A. Turner, Executive Director, Information Services Executive Council, *The Impact of Data Restrictions On Consumer Distance Shopping,* 2001.
[2] Ernst & Young LLP, *Customer Benefits from Current Information Sharing by Financial Services Companies,* conducted for The Financial Services Roundtable, December 2000.
[3] Walter F. Kitchenman, Senior Analyst, Commercial Banking, The Tower Group, *Summary of Tower Group Studies Related to European System of Opt-In,* 1999
[4] Fred H. Cate, Professor of Law and Director of the Information Law and Commerce Institute, Indiana University School of Law, Michael E. Staten, distinguished Professor and Director of the Credit Research Center, The Robert Emmett McDonough School of Business, Georgetown University, *Putting People First: Consumer Benefits of Information-Sharing: Summary,* December 2000
[5] Fred H. Cate, Professor of Law and Director of the Information Law and Commerce Institute, Indiana University School of Law, Michael E. Staten, distinguished Professor and Director of the Credit Research Center, The Robert Emmett McDonough School of Business, Georgetown University, *Putting People First: Consumer Benefits of Information-Sharing,* December 2000
[6] Ernst & Young LLP, *Customer Benefits from Current Information Sharing by Financial Services Companies,* conducted for The Financial Services Roundtable, December 2000.
[7] Walter F. Kitchenman, Senior Analyst, Commercial Banking, The Tower Group, *Summary of Tower Group Studies Related to European System of Opt-In,* 1999.
[8] WEFA Group, *2000 Economic Impact: U.S. Executive Marketing Today Executive Summary,* http://www.the-dma.org/library/publications/libres-ecoimp1b1a.shtml
[9] Fred H. Cate, Professor of Law and Director of the Information Law and Commerce Institute, Indiana University School of Law, Michael E. Staten, distinguished Professor and Director of the Credit Research Center, The Robert Emmett McDonough School of Business, Georgetown University, *The Value of Information-Sharing,* July 2000.
[10] Walter F. Kitchenman, Senior Analyst, Commercial Banking, The Tower Group, *US Credit Reporting: Perceived Benefits Outweigh Privacy Concerns,* January 1999
[11] Ernst & Young LLP, *Customer Benefits from Current Information Sharing by Financial Services Companies,* conducted for The Financial Services Roundtable, December 2000.
[12] Fred H. Cate, Professor of Law and Director of the Information Law and Commerce Institute, Indiana University School of Law, Michael E. Staten, distinguished Professor and Director of the Credit Research Center, The Robert Emmett McDonough School of Business, Georgetown University, *The Value of Information-Sharing,* July 2000.
[13] Michael A. Turner, Executive Director, Information Services Executive Council, *The Impact of Data Restrictions On Consumer Distance Shopping,* 2001.
[14] Paul H. Rubin and Thomas M Lenard, The Progress & Freedom Foundation, *Privacy and the Commercial use of Personal Information,* July 2001.

Mr. STEARNS. Thank you. Ms. Zuccarini, I have a question. You talk about these myths that you mentioned. You have a national fraud data base, though, right?

Ms. ZUCCARINI. Yes, we do.

Mr. STEARNS. And why was it established? And isn't it oriented toward individuals?

Ms. ZUCCARINI. It is, but that is not a marketing use. It is not for marketing purposes.

Mr. STEARNS. Why was it established?

Ms. ZUCCARINI. To help prevent identity fraud, and detect fraud.

Mr. STEARNS. And who gets access to that?

Ms. ZUCCARINI. That would be businesses that have a need for that. That is not a marketing purpose, and covered under the——

Mr. STEARNS. So a business could subscribe to this? Any business could subscribe to this fraud data base?

Ms. ZUCCARINI. I am not positive of the answer to that. I would have to get back to you. It is in a different division.

Mr. STEARNS. Okay. When you go on the Internet, you see these web sites that say, we go and get credit information. We go to public courthouses, and we go across the board, and find all this information, and we compile it. Does your company do that?

Ms. ZUCCARINI. We do that in a separate division.

Mr. STEARNS. Okay. And then you provide this information for law enforcement, government agencies, and you say "other organizations with legitimate and appropriate need for such information," I think you are indicating.

Ms. ZUCCARINI. Other qualified users, such as——

Mr. STEARNS. Yes. What other organizations would have access besides law enforcement, government agencies, and how would they get it?

Ms. ZUCCARINI. It would have to be a purpose that would be covered under the Fair Credit, or the exemptions to the Fair Credit Reporting Act. In terms of examples of users, I believe I gave some in my written testimony: child support enforcement, witness look-up and protection, those types of things.

Mr. STEARNS. In your testimony, you indicated that Experian has found that "rigid rules directing information use are quickly outdated by today's rapidly evolving technology and constantly changing consumer and business needs and expectations." You might just help us with what you mean by that, how it has changed, and you know, what impact that would have, from our standpoint as a legislator.

Ms. ZUCCARINI. Experian has five core information values that we live by and we practice within our business: balance, accuracy, security, integrity, and communication. We have privacy compliance teams within each business unit that are responsible for enforcing these values and the written policies that support them.

By ensuring that our entire organization is aware of these five values—in addition to written policies and the officers that are responsible for making sure that they are employed—that gives us flexibility in making sure that we are recognizing whether technologies are advancing, or there are different needs to protect certain types of sensitive data, for example.

Mr. STEARNS. Okay. Ms. Barrett, you make the point that "e-commerce has increased consumer product availability. It has also made consumer recognition more difficult." What do you mean by that?

Ms. BARRETT. Well, I will go back to the example I used earlier of the store owner of 100 years ago, where he knew his customer because he walked in. Today, many customers buy from the Internet, they buy over the telephone, or they order through a catalogue, and the merchant has no opportunity to interact with that customer beyond the purchase.

That makes it much more difficult for a company to really understand, beyond what a customer bought, who that customer is, what they are interested in, what other products and services might be of likely interest.

Mr. STEARNS. Going back to this web site, where you can pay $35 and find this information that Mr. Doyle talked about—you know, if a corporation came to you and said, we want to buy this information, or—you would give him this information, he might put it on the web site. How do you protect the consumer whose information you have?

Ms. BARRETT. We have a variety of products that are designed and developed for very specific business purposes. We do not sell data in bulk to anyone for any purpose. Our contracts limit what the data can be used for by the purchaser, and we monitor that to assure that those contractual restrictions are enforced.

Mr. STEARNS. Mr. Ford, you highlight that "the harm of using personal information practices for marketing is minimal." Can you describe the harm that such information, I guess—how can it be

misused, or how do you go to protect so that the marketing information would be misused? Did that make sense?

Mr. FORD. Let me make sure I understand your question, Mr. Stearns. Are you asking me to define some ways in which marketing data might be misused?

Mr. STEARNS. You are saying it is minimal. Give me examples of how it would be misused, and what you are doing to protect it, so that you don't have that case.

Mr. FORD. I think one example comes in the use of the information that we have. For example, what restrictions do we place on who is able to receive that information? We, for example, have a policy that we do not provide certain data to insurance companies. We make sure that when a subscriber, or someone who uses our data, we have policies and procedures in place that allow us to check and make sure that the information we have provided is only being used in accordance with the contract.

We have review authority for any of the copy or the direct marketing materials that go out. So we are in a position to take a look at what our customers are doing with the data that we provide.

Mr. STEARNS. You mentioned that you have undergone privacy audits conducted by Dr. Westin?

Mr. FORD. Correct.

Mr. STEARNS. And can you explain how, how comprehensive are these audits? And what standards do they meet? Is there a seal of approval or best business practices-type of thing? And what is the cost of such an audit?

Mr. FORD. Okay, that is a great question, I appreciate your asking it. Without sounding too flippant, we like to say at Equifax that we were for privacy before privacy was cool. We engaged Dr. Alan Westin in 1988 as a privacy consultant for us.

Since that time, he has helped us develop our privacy policies and our procedures. And he has developed, with our input, too, a template that we use, that we overlay for each product or service before it goes out the door. And in fact, the template has evolved to where it covers issues like notice, and choice, and access, and security, and the standard fair information practices that I think we are all accustomed to.

So we have an internal process in our company that forces our products and services to go through this review before it goes to the marketplace.

Mr. STEARNS. And what does it cost, such an audit?

Mr. FORD. Alan Westin is on retainer, annual retainer to us. This is part of his consulting assignment for us.

If I might add, too, sir, we also were one of the first companies to qualify for and earn the Better Business Bureau Online Privacy seal. So in terms of audit, in terms of consumers going to our web site—I think the previous panel mentioned a visible way of generating trust and confidence at the site; having that seal up there is one way to do that.

Mr. STEARNS. Okay. My time has expired. Mr. Towns?

Mr. TOWNS. Thank you very much, Mr. Chairman. I think all of you, I think I hear you saying that self-regulation is the key to your business growth and development. And I trust and do believe

that all of you are good actors and so on, in terms of you doing things right.

Would your organizations support a bill which would create financial penalties for companies who commit online fraud and abuse? Go right down the line, starting with Ms. Barrett.

Ms. BARRETT. Okay. We believe that online fraud and abuse is already illegal, and certainly would support any legislation that strengthens those penalties.

Mr. TOWNS. Mr. Ford? I know you say that harm is minimal, but——

Mr. FORD. Well, I agree with Ms. Barrett that the fraud and deterrence act that was passed a couple of years ago was a bill that Equifax supported. I think your larger question might be would we support further legislation, and I don't mean to put the question in my words. But it is not a perfect world, and I don't think there is such a thing as perfect legislation. So our view, Equifax's view, is that we would like to see self-regulation be given a chance to run its course. If it doesn't work, and there is an actual, demonstrated, real harm, then let's focus on legislation that would address that particular harm.

Mr. TOWNS. Yes, I was thinking that the bad actors that would be punished, while still being held to some kind of minimum standards. I am a little concerned about not having one.

Mr. FORD. Again, sir, I would say that if responsible companies do business with responsible companies, then those bad actors ultimately are going to be weeded out of the marketplace.

Mr. TOWNS. Ms. Zuccarini?

Ms. ZUCCARINI. I would agree with Jennifer and John, that online fraud, we believe, is already illegal, and prosecuting that should definitely be encouraged.

With regard to additional legislation, we too believe that the record is not yet clear whether there are unintended consequences that might come from restricting further use of marketing information, and what the impact might be, both on businesses and on consumers, in terms of choice.

Mr. TOWNS. Well, you know, you are right, I mean, it is illegal. But you know, but it is being done. And I am not sure how much—you said "minimal," but I am not sure in terms of how much is going on.

But let me ask this: how secure are your data bases? How certain are you that you can prevent unauthorized access?

Ms. ZUCCARINI. Question for me?

Mr. TOWNS. I am going down the line.

Ms. ZUCCARINI. Sure, I can take that. We have been responsible stewards of consumer information for over 50 years. Making sure consumer information is secure is mission-critical for Experian.

We have a variety of different security techniques that range from our general security environment of being password-protected with encrypted data transfer, to requiring IDs with security cameras. We have automated system monitoring that indicates what type of data is being accessed and when and by whom. We have automated and manual systems that flag when sensitive data is being accessed, and bring transactions to a halt until we can actually manually inspect that and approve it.

In addition to that, we have contractual requirements in our contracts that state that the data must be used for marketing purposes; that we have the right to inspect any communication associated with it. We have the right to audit, and we do business with legitimate businesses.

Mr. FORD. I don't know that there is much I could add to that. That covers the gamut for Equifax as well, in terms of the physical security, in terms of the technological security, in terms of—maybe one thing I could add is let's remember that most of this data, even if someone were to be able to get access to it, most of this data is probability data. It is characteristics about a particular zip code or geographic area, for example.

The data is not organized by name. So it is not as if there is an Equifax direct marketing file for John Ford, and there is this little pigeonhole, and all this data about me is in there. The file is not organized that way.

Ms. BARRETT. I would concur with the comments from Mr. Ford and Ms. Zuccarini. I might add that Acxiom also employs external auditors, security auditors, to come in on a regular basis to test our processes and our systems to make sure they are current with technology and the latest security updates.

Mr. TOWNS. Right. Is any opportunity provided for a person to make a request, that I would like to come in and review, you know, my files with you? Is it possible for that to happen?

Ms. BARRETT. We do not provide access to our marketing information. Our systems are not designed in a way that you can go in and look up information on one individual. If a consumer contacts us and is interested about what information we have on them, we tell them what types of information we might have in the data base, and if they are uncomfortable with that, we offer them the opportunity to opt out of that data base.

Mr. FORD. Again, Mr. Towns, the data base is not organized by name and address. So it would take a programmer to go in and obtain the personally identifiable data, name and address, and then associate the characteristics that we ascribe to that person in some kind of file. So yes, it can be done, but it is not a feasible process at the moment.

Ms. ZUCCARINI. I would echo their comments. First of all, our data is not in any single giant data base. It is in multiple places. We have no mechanism as well to provide access. If a consumer comes to us with questions about information we may have about them, we also describe the type of information that we have and offer them the opportunity to opt out.

Mr. TOWNS. Well, let me make sure I understand this. I mean, this is a complicated issue.

Ms. ZUCCARINI. Yeah.

Mr. TOWNS. Okay. I'm happy that I'm not alone.

If you don't have it by individual, how can a person opt out?

Ms. BARRETT. The data is actually stored in large files that are not accessible by individual record.

Mr. TOWNS. Then how can I opt out?

Ms. BARRETT. The files are updated and maintained on a batch basis. And the ability to opt out occurs when maintenance trans-

actions are applied to those files. It is not a look-up type of service that allows you to go retrieve the data on an individual.

Mr. FORD. If I can interject, I think maybe another way to look at it is the outcome of the process by which a customer of ours obtains data is a list of name and addresses. Before that list goes anywhere, we run it up against any opt-out list—our own, or whether it is the Direct Marketing Association's list—to take those names out at the back end of the process. That is how people can opt out.

Mr. TOWNS. I guess by now you know that there is a tremendous amount of pressure from a lot of us, from our consumers, you know, to really take a very serious look at this and do something. And there are complaints; every time I have a town hall meeting, you know, I always get one person—and the funny thing about this is that one person can tell a story and there comes a situation where everybody wants to top it. And this goes on, and it gets bigger and bigger.

So it is at the point where I really feel that Congress has to take some kind of action. And I am happy that the chairman is moving very slowly, because I wouldn't want to just jump and do something. We are hearing from a lot of folks; I think that is important.

But eventually, I really feel that we will have to take some kind of action. And I don't want to do anything that is going to jeopardize any company's ability to continue to grow and to expand. But at the same time, we need to reassure our consumers, the clients out there, and our constituents, that there is this kind of protection in terms of privacy.

Every now and then things happen. I will give you an example. I played at a golf course not too long ago. I mean, I don't even play a lot of golf; I just signed up, went out there and banged away. And now I am getting all this material. Now, I realize that it is from playing at that golf course.

I don't want this material. I don't want anything. I don't want to know anything about it, because I don't ever plan to go back there again. So, you know, these are the kinds of things that when you hear this, you know that these things are going on.

And I don't question for a moment the fact that you are doing the right thing. But my problem is, is with those that are not doing the right thing, and that I am not sure the penalties are great enough, or strong enough, to really give the kind of protection that we need to give.

And that is where I am coming from. I don't question anything you have said today in reference to your companies. I do believe you are doing the right thing. But you must know, too, there are some folks out there that are not doing the right thing, and that is our problem. That is our problem. And they make it bad for you as well.

Mr. Chairman, on that note I yield.

Mr. STEARNS. Okay. We can go a second round. I just have some illustrative points along where my colleague from New York brought this discussion. Experian has, in Appendix B to their testimony—and I just want to list some of the things that they seek, in terms of marketing data.

They go to public records, and they go to white page telephone listings, to get information. And then they go to real estate information—your home ownership, the type of home you have, the characteristics. They go to voter records—name, address, date of birth. They go to occupational licenses, State professional licenses, whether it be medical, attorney, cosmetology. Then they will go to recreational license, to see if you have a fishing license or a hunting license.

Then, if they have back from you a card that you have filled out—perhaps you filled this card out because you want to get a new car, or you want to get a free gift—they would have lifestyle information. They would have, you know, things that you enjoy—whether it is sports, music, investing, hobbies, great outdoors, world environment. And then it gets to your age, your marital status, gender, home ownership, number of children. And they ask for an estimated home income.

Now, you take all that information and you try and correlate it with the census information, which doesn't have the name, but does have a lot of information that you filled out. You can get a pretty good picture of a person. Am I wrong? Is that true, that with this kind of data base, that the Americans who are, I think, unaware of the kind of information that you would have—and you say it is not for individual, but it is provided with a name with it.

Ms. ZUCCARINI. That is correct, it is. It is demographic, lifestyle, and interest information. And the lifestyle and interest information is either self-reported or public record data.

Mr. STEARNS. Now, let's say I want to get a copy of everything you have on me. How would I do it?

Ms. ZUCCARINI. We wouldn't provide that to you, because we have a policy of not providing data to individuals.

Mr. STEARNS. Okay. Yet you could sell that information—and I am not being critical; I am just exploring this for whoever is interested. A non-profit organization could come to you and say, you know, I want to buy this from you. You would sell it to a not-for-profit organization, wouldn't you?

Ms. ZUCCARINI. We would sell a list.

Mr. STEARNS. A list?

Ms. ZUCCARINI. Of no less than 50. Our systems don't even return a list of under 50.

Mr. STEARNS. Okay. And so I would have to specify all these lifestyle characteristics and the information in here to get the list? But you would not provide individual names correlated with all this information?

Ms. ZUCCARINI. We would provide a list back to you that had a list of people that satisfied your request for different lifestyle interests.

Let's say, if you were interested in selecting people that enjoy cooking, because you have a cooking catalogue, you would get back a list of individuals that enjoy cooking.

Mr. STEARNS. So I could come to you and say, okay, I want somebody who is making between $50,000 and $100,000 who is interested in rhythm and blues music, who enjoys skiing, who has a fishing license, and attends church, and also interested in gar-

dening, and is married with three children. You could come back with a list?

Ms. ZUCCARINI. We could come back with a list, yes.

Mr. STEARNS. And you would give me names?

Ms. ZUCCARINI. We would. So you could send an advertising offer to them. For marketing purposes.

Mr. STEARNS. Now, let's say a person is in your data base and he or she wants to get out of that data base. How do they get out?

Ms. ZUCCARINI. A variety of different ways. We honor the Direct Marketing Association mail preference service and telephone preference services and e-mail preference services, which are widely publicized, which allow people to go directly to the DMA—they don't even have to contact us.

We publicize, on our web site and with a toll-free phone number, that you can call, if you would like to remove yourself from our mailing list. In addition, we provide consumer advocate groups, legislators, States' attorney general's offices, a variety of different groups, with an extensive consumer outreach program, where we outline the steps that you can take to remove yourself from our marketing information list.

Mr. STEARNS. Okay. What would be your worst nightmare? For example, Ms. Barrett, your company makes most of its money dealing with the management of these data bases. And I assume, certainly Experian is, you're owned by Europe, by a European company.

Ms. ZUCCARINI. We are owned by Great Universal Stores.

Mr. STEARNS. Yes, so you are over in Europe. Does that mean you are complying with the European Internet privacy——

Ms. ZUCCARINI. Our international operations are largely autonomous. We are compliant with the country laws in Europe. We have not subscribed to safe harbor.

Mr. STEARNS. You have not subscribed?

Ms. ZUCCARINI. No, we have not.

Mr. STEARNS. But since you are a European Union company, I would think you would have to comply.

Ms. ZUCCARINI. Our U.K. operations, our international operations. I am talking about Experian Marketing Solutions, the organization that I am representing today here in the U.S.

Mr. STEARNS. Oh, okay. Okay, I see that. So the worst nightmare would be, Ms. Barrett, for your company, is if the Federal Government came up with this Internet privacy legislation like the European Union's, so that your data bases would be affected, don't you think?

Ms. BARRETT. Well, in that we operate in five countries in Europe as well as here in the United States, we appreciate the differences between the European law and the U.S. law.

Mr. STEARNS. Right. I am just trying to help you out. You are trying to tell us as legislators, please, Mr. Legislator, don't do this, because this would harm us because we get most of our income from the management of these data bases. So I am just trying to understand from your point of view, as I try to understand for consumer groups—when they come in here, I ask them the same question: what is the thing that concerns you most? What should I do as a legislator, and Mr. Towns, and so on?

And so I am asking you, what would be your concern if we developed an Internet privacy bill that would, you know, do something with the data bases that you manage?

Ms. BARRETT. If it restricted the flow of information for legitimate businesses to use for marketing purposes, then not only Acxiom but our customers, and ultimately the consumers, are going to have serious economic impacts. A number of studies show the variety of economic benefits and savings that our customers, through the use of our data, get. An apparel study showed that somewhere between 3 and 11 percent, if you restricted in the way that the Europeans have, some of the data, the costs in the apparel industry would go up between 3 and 6 percent. We view that really as a means of taxing the consumer to pay for the lack of economic benefit that we enjoy today.

Mr. STEARNS. Mr. Ford? Either one of the other panelists would like to comment, what would be your worst nightmare?

Mr. FORD. I haven't given it a great deal of thought. But in the past minute, I would have to say that probably mandated opt-in—and I am speaking about off-line and online.

Mr. STEARNS. Now, there are a lot of people that want to do a mandated opt-in. Particularly with financial and medical records.

Mr. FORD. Well, that is a different story, because in the direct marketing business that we are talking about, we don't have financial records or medical records. We are only talking about the kind of direct marketing information that we have. I think what you are about ready to refer to is ailment data that is self-reported by the consumer.

Mr. STEARNS. The problem is that people say, well, just financial or medical information is sensitive. But if you take all this information that I mentioned here, in terms of the lifestyle, and then you combine that with public records and telephone directory information, and then the census information that I can glean from your neighborhood and where you live, you come up with some pretty sensitive information about individuals. And maybe people want to be able to opt in.

Mr. FORD. Well, I would ask that you remember, sir, that the kind of information that is sensitive there is self-reported information. It is not information that my company goes out and gleans from someplace.

Mr. STEARNS. No, I understand.

Mr. FORD. So there is a built-in—there is a built-in opt-in, if I am filling out——

Mr. STEARNS. Because they volunteered?

Mr. FORD. Because they volunteered the information. And we make it possible for them to opt out of what they have opted into. They can come back later on and say, no, I want to take that back.

In fact, on our web site, which conducts this same kind of survey, there is a double opt-in. They fill out the survey, they are asked if they are comfortable with it, if they really want to send it. They hit the button, yes, they do, we come back at them and say, "Are you sure?" And then, each time we ask them to fill out the survey again, they have the ability to unsubscribe.

So I submit that the sensitive information, such as it is, is voluntarily provided.

Mr. STEARNS. Anything you would like to add to that? What your worst nightmare is?

Ms. ZUCCARINI. My worst nightmare? I have many nightmares, but my worst one is mandated opt-in, because I think what we are doing then is setting the default standard for the majority of the population, whether we are looking at opt-in or opt-out. And if we are looking at opt-in, then we believe that that default standard will be not so much a sincere concern about protection of privacy, but may be as a result of consumer inertia, people not wanting to respond back affirmatively. And we are concerned about the potential unintended consequences, again, both economically and to consumers in terms of less choice, higher prices, and less competition.

What you would start to look at in that case is an extreme challenge for a new market entrant or a small business to actually be able to compete and advertise effectively.

Mr. STEARNS. Yes, Mr. Ford?

Mr. FORD. May I make one more comment about that, sir?

Mr. STEARNS. Sure.

Mr. FORD. I think that we are all in agreement that we want consumers to have informed choice. And we do both; at Equifax, we provide the ability for consumers to opt out of this data off-line, and we provide online the ability to opt in.

But I think there are a number of national surveys who have kind of segmented the American population into a group that is called privacy fundamentalists, a group that is probably 20 percent or so, maybe more, 20, 25 percent, at one end that are privacy fundamentalists. At the other end, you have the privacy unconcerned, maybe 15 percent.

Mr. STEARNS. Libertarians.

Mr. FORD. And then in the middle, you have got this 55 percent that are the pragmatic middle. So we need a system that satisfies the needs of that full range of people who want to have different choices.

By making opt-in the default mechanism, we satisfy probably the privacy fundamentalists, and we disenfranchise the other two-thirds who may want to see those offers. They may want to become informed citizens by receiving these offers. So my argument is, let's go with an opt-out mechanism. It still protects the fundamentalists who want to not receive any more, and it offers the choice to the other two-thirds.

Mr. STEARNS. Well, I think—Mr. Towns?

Mr. TOWNS. Yes. Well, you know, I want to go back to the bad actors. You know, they are out there. What should we do about them? Because what is going on now is really not working. It is not that effective. So what do we do to sort of address that issue? Other than pray?

Mr. FORD. That, too.

Ms. BARRETT. Mr. Towns, I think we have—if there is any area for criticism, both of the government and of industry, is that we have not done a good job of educating the consumer about not only what their choices are, but how to watch out for bad actors.

There are many things that industry is working on in that regard. I think individual companies need to take the initiative as well. We have produced a booklet called "What Every Consumer

Should Know About the Use of Personal Information." It is available on our web site. We would love to have it distributed by anyone who wants to distribute it.

I think that we have an obligation and a responsibility to consumers to tell them about not only the valuable uses of information, but the tools and choices that they have at their hands, so that those that do want to exercise them can.

Mr. TOWNS. The accuracy in your data base, do you feel comfortable with that? In terms of the accuracy, do you think it is very accurate?

Ms. BARRETT. We strive very hard to make the data in our data bases accurate. And in our interactions with consumers, we actually have consumers that contact us and have learned that it is inaccurate, and give us corrected information. So we are always striving to keep the data accurate and current.

Mr. FORD. Perhaps a better word for us is, is the data base reliable? Is it predictive? Can our customers use it reliably to make sure that they are sending the kind of offers to the kind of people who are interested in receiving those offers? And I think our data bases are highly reliable.

Ms. ZUCCARINI. We would concur with that as well. We put an enormous amount of resources and effort against making sure that the information is as accurate as we can make it, and making sure as well that it is reliable, so that businesses, again, can try to determine whether consumers are interested in receiving marketing offers.

Mr. TOWNS. Mr. Ford and Ms. Zuccarini, I still want to get your views and feelings on what we should do about these bad actors.

Ms. ZUCCARINI. Can I comment on that?

Mr. FORD. Go ahead.

Ms. ZUCCARINI. Yes, again, our first recommendation would be, make sure that we are strictly enforcing the existing laws. There are, I believe, eight laws at least that currently govern the type of marketing information that we are discussing today. In addition to that, we have very strict self-regulatory guidelines through our trade organizations, and our clients are members of those. And to make sure that we are doing that, and really step up the enforcement.

The second thing would be to echo what Ms. Barrett said with regard to consumer education. We need to do a better job of making sure consumers understand how to recognize bad actors, and how they can contribute to making sure that they are no longer in business.

Mr. FORD. I look at it as a three-pronged initiative, or three sets of responsibilities. Business has a responsibility to educate consumers about the products and the services, and the technologies that are out there that they can use to help them protect their privacy.

Government has a responsibility in two ways. No. 1, to enforce the laws that have already been enacted. And No. 2, I think that on the political side, that peeling this onion, which this series of hearings is really trying to do, to understand the complexities of this issue, is very, very important to making good public policy. And that is what you are doing, and I very much appreciate that.

On the consumer side, though, they have an obligation and a responsibility, I think, as well, to make themselves informed consumers; to take advantage of the information that is out there, the products, the technologies.

And there is also something known as the teachable moment: to send out some educational material to a consumer who is not at a teachable moment is not very effective. So finding those opportunities when consumers are, if not eager, at least willing to learn more, is a task that business must set itself, too.

Mr. TOWNS. Thank you very much. Thank you, Mr. Chairman.

Mr. STEARNS. I thank my colleague. We will complete the second panel. We want to thank you, again, for waiting for us. We had a very good hearing, and I think, as you pointed out, that we are moving incrementally to try to understand this very broad and significant and comprehensive area. And we thank you again for testifying.

And the subcommittee is adjourned.

[Whereupon, at 12:55 p.m., the subcommittee was adjourned.]