EXPLORING THE OFFLINE AND ONLINE COLLECTION AND USE OF CONSUMER INFORMATION

JOINT HEARING

BEFORE THE

SUBCOMMITTEE ON COMMERCE, TRADE, AND CONSUMER PROTECTION

AND THE

SUBCOMMITTEE ON COMMUNICATIONS, TECHNOLOGY, AND THE INTERNET

OF THE

COMMITTEE ON ENERGY AND COMMERCE

HOUSE OF REPRESENTATIVES

ONE HUNDRED ELEVENTH CONGRESS

FIRST SESSION

NOVEMBER 19, 2009

Serial No. 111–83

Printed for the use of the Committee on Energy and Commerce

energycommerce.house.gov

U.S. GOVERNMENT PRINTING OFFICE

74–854 WASHINGTON : 2012

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) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON ENERGY AND COMMERCE

HENRY A. WAXMAN, California, *Chairman*

JOHN D. DINGELL, Michigan
Chairman Emeritus
EDWARD J. MARKEY, Massachusetts
RICK BOUCHER, Virginia
FRANK PALLONE, JR., New Jersey
BART GORDON, Tennessee
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
BART STUPAK, Michigan
ELIOT L. ENGEL, New York
GENE GREEN, Texas
DIANA DEGETTE, Colorado
Vice Chairman
LOIS CAPPS, California
MICHAEL F. DOYLE, Pennsylvania
JANE HARMAN, California
TOM ALLEN, Maine
JANICE D. SCHAKOWSKY, Illinois
HILDA L. SOLIS, California
CHARLES A. GONZALEZ, Texas
JAY INSLEE, Washington
TAMMY BALDWIN, Wisconsin
MIKE ROSS, Arkansas
ANTHONY D. WEINER, New York
JIM MATHESON, Utah
G.K. BUTTERFIELD, North Carolina
CHARLIE MELANCON, Louisiana
JOHN BARROW, Georgia
BARON P. HILL, Indiana
DORIS O. MATSUI, California
DONNA M. CHRISTENSEN, Virgin Islands
KATHY CASTOR, Florida
JOHN P. SARBANES, Maryland
CHRISTOPHER S. MURPHY, Connecticut
ZACHARY T. SPACE, Ohio
JERRY MCNERNEY, California
BETTY SUTTON, Ohio
BRUCE L. BRALEY, Iowa
PETER WELCH, Vermont

JOE BARTON, Texas
Ranking Member
RALPH M. HALL, Texas
FRED UPTON, Michigan
CLIFF STEARNS, Florida
NATHAN DEAL, Georgia
ED WHITFIELD, Kentucky
JOHN SHIMKUS, Illinois
JOHN B. SHADEGG, Arizona
ROY BLUNT, Missouri
STEVE BUYER, Indiana
GEORGE RADANOVICH, California
JOSEPH R. PITTS, Pennsylvania
MARY BONO MACK, California
GREG WALDEN, Oregon
LEE TERRY, Nebraska
MIKE ROGERS, Michigan
SUE WILKINS MYRICK, North Carolina
JOHN SULLIVAN, Oklahoma
TIM MURPHY, Pennsylvania
MICHAEL C. BURGESS, Texas
MARSHA BLACKBURN, Tennessee
PHIL GINGREY, Georgia
STEVE SCALISE, Louisiana
PARKER GRIFFITH, Alabama
ROBERT E. LATTA, Ohio

SUBCOMMITTEE ON COMMERCE, TRADE, AND CONSUMER PROTECTION

BOBBY L. RUSH, Illinois
Chairman

JANICE D. SCHAKOWSKY, Illinois
Vice Chair
JOHN P. SARBANES, Maryland
BETTY SUTTON, Ohio
FRANK PALLONE, JR., New Jersey
BART GORDON, Tennessee
BART STUPAK, Michigan
GENE GREEN, Texas
CHARLES A. GONZALEZ, Texas
ANTHONY D. WEINER, New York
JIM MATHESON, Utah
G.K. BUTTERFIELD, North Carolina
JOHN BARROW, Georgia
DORIS O. MATSUI, California
KATHY CASTOR, Florida
ZACHARY T. SPACE, Ohio
BRUCE L. BRALEY, Iowa
DIANA DEGETTE, Colorado
JOHN D. DINGELL, Michigan (ex officio)

CLIFF STEARNS, Florida
Ranking Member
RALPH M. HALL, Texas
ED WHITFIELD, Kentucky
GEORGE RADANOVICH, California
JOSEPH R. PITTS, Pennsylvania
MARY BONO MACK, California
LEE TERRY, Nebraska
MIKE ROGERS, Michigan
SUE WILKINS MYRICK, North Carolina
MICHAEL C. BURGESS, Texas

SUBCOMMITTEE ON COMMUNICATIONS, TECHNOLOGY, AND THE INTERNET

RICK BOUCHER, Virginia
Chairman

EDWARD J. MARKEY, Massachusetts
BART GORDON, Tennessee
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
BART STUPAK, Michigan
DIANA DEGETTE, Colorado
MICHAEL F. DOYLE, Pennsylvania
JAY INSLEE, Washington
ANTHONY D. WEINER, New York
G.K. BUTTERFIELD, North Carolina
CHARLIE MELANCON, Louisiana
BARON P. HILL, Indiana
DORIS O. MATSUI, California
DONNA M. CHRISTENSEN, Virgin Islands
KATHY CASTOR, Florida
CHRISTOPHER S. MURPHY, Connecticut
ZACHARY T. SPACE, Ohio
JERRY MCNERNEY, California
PETER WELCH, Vermont
JOHN D. DINGELL, Michigan (ex officio)

FRED UPTON, Michigan
Ranking Member
CLIFF STEARNS, Florida
NATHAN DEAL, Georgia
BARBARA CUBIN, Wyoming
JOHN SHIMKUS, Illinois
GEORGE RADANOVICH, California
MARY BONO MACK, California
GREG WALDEN, Oregon
LEE TERRY, Nebraska
MIKE FERGUSON, New Jersey

CONTENTS

WITNESSES

SUBMITTED MATERIAL

EXPLORING THE OFFLINE AND ONLINE COLLECTION AND USE OF CONSUMER INFORMATION

THURSDAY, NOVEMBER 19, 2009

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON COMMERCE, TRADE, AND CONSUMER PROTECTION,
JOINT WITH THE
SUBCOMMITTEE ON COMMUNICATIONS, TECHNOLOGY, AND THE INTERNET,
COMMITTEE ON ENERGY AND COMMERCE,
Washington, DC.

The Subcommittees met, pursuant to call, at 12:23 p.m., in Room 2123 of the Rayburn House Office Building, Hon. Bobby Rush [Chairman of the Subcommittee on Commerce, Trade, and Consumer Protection] presiding.

Members present from Subcommittee on Commerce, Trade, and Consumer Protection: Representatives Rush, Schakowsky, Sarbanes, Green, Barrow, Matsui, Space, Radanovich, and Scalise.

Members present from Subcommittee on Communications, Technology, and the Internet: Representatives Boucher, Markey, Doyle, Inslee, Murphy, McNerney, Stearns, Shimkus, and Blackburn.

Staff Present: Michelle Ash, Chief Counsel; Marc Groman, FTC Detailee; Timothy Robinson, Counsel; Amy Levine, Counsel; Greg Guice, FCC Detailee; Sarah Fisher, Special Assistant; .Will Cusey, Special Assistant; Theresa Cederoth, Intern; Pat Delgado, Rep. Waxman's Chief of Staff; Brian McCullough, Senior Professional Staff; Shannon Weinberg, Counsel; Will Carty, Professional Staff; Amy Bender, FCC Detailee; and Sam Skywalker Costello, Legislative Analyst.

OPENING STATEMENT OF HON. BOBBY L. RUSH, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF ILLINOIS

Mr. RUSH. The joint committee will come to order.

This is a joint subcommittee hearing on Commerce, Trade, and Consumer Protection, and the Commerce, Technology, and Internet Subcommittee.

The subject matter for this hearing is entitled "Exploring the Offline and Online Collection and Use of Consumer Information." I am privileged to chair the Subcommittee on Commerce, Trade, and Consumer Protection, and my friend and colleague, Mr. Boucher, who is the chairman of the Communications, Technology, and

Internet Subcommittee of the Committee on Energy and Commerce.

It is my honor to chair the first part of this hearing, and this hearing will be chaired subsequently by Chairman Boucher. The chair recognizes himself now for 5 minutes, for the privileges and the purposes of an opening statement.

The collection and use of personal information of customers and consumers are threads from the same knitting needle, sewn into the fabric of American commerce and competition near the start of the Twentieth Century. Accordingly, these tools and methods predate their more powerful, precise, and predictive counterpart in the online realm by more than 100 years.

But just because we have something that has been around for a long time does not mean we understand as much about it as we should. That is why I am delighted about today's hearing. It is the fourth in a series of hearings our two subcommittees have held on the subject of privacy.

At our hearings and in our meetings, consumers and their advocates, industry, and leading commentators have shared with us extensively why this all matters, how entrepreneurs and businesses go about protecting consumer privacy, and why collecting personal information about individual consumers improves the chances their businesses will have to succeed. While preparing for these hearings, we have been surprised at how little is really known about how businesses go about ensuring that individual privacy is protected.

Consumers are telling us they want to know more about how their information is being protected. As their representatives and consumers ourselves, we hear them loud and clear. They should be and are concerned, even to the point of anger, when they learn that they have been placed on consumer lists identifying themselves as affluent Jews or Blacks, as pro-choice or pro-life, as donors, as members of a same-sex couple relationship, or as being addicted to gambling, addicted or sex, or addicted to tobacco.

Indeed, on my way back home to Chicago to celebrate the Thanksgiving holidays, I could take public transportation to the airport, and by using a SmartCard and a frequent flyer card, records of my whereabouts, and when and to where I was commuting and flying are created. To buy my holiday turkey, I may use my grocery rewards card, which would swipe into a system of databases what is in my cart, when and where I shopped, how much I paid, among the other data points that were being collected. And these are just several examples of the type of consumer lists and data points that are generated and populated into databases, 24 hours a day, 365 days of every year.

But how much do we know about the businesses that make it a business of obtaining and selling or sharing "offline" information and customer lists with affiliated and unaffiliated businesses. How much do we know about their marketing practices and product development strategies to persuade buyers and individuals who will pay considerable amounts of money for that information? How much do we really know about what these buyers and individuals do with that information, including reselling the information downstream to other buyers and bidders for that information?

I am interested in hearing everyone's perspectives about the current legal and regulatory structure that exists to protect this information. Should the source of this information, whether it is taken "offline" from a warranty registration card, or "online," from a social or health networking site be treated differently, when it reveals fundamentally the same personal information about individual consumers? And by treating the information differently, with a heightened duty on businesses to protect "online sources," for example, are we setting perverse incentives and conditions for regulatory arbitrage and avoidance?

Let me be clear. My end goal is to work with members of this subcommittee and members of this committee to introduce privacy legislation, which protects consumers from privacy-related harms, yet doesn't stifle responsible entrepreneurs and businesspeople from developing models and instituting successful business and marketing plans that are, indeed, respectful of consumer privacy.

Keeping privacy protections that belong in the back office from tumbling into the crawl spaces under the office will be a big part of our challenge. In whatever bill we draft, we must work to ensure that the accelerating convergence of "offline" and "online" collection does not outpace the demands of consumers for dignity and for discipline and for our decency, in our dawning digital economy and markets.

I yield back the balance of my time.

Mr. RUSH. I recognize the ranking member of this subcommittee, Mr. Radanovich, for 5 minutes for the purposes of opening statements.

OPENING STATEMENT OF HON. GEORGE RADANOVICH, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA

Mr. RADANOVICH. Thank you, Chairman Rush, and I want to thank you for holding this second hearing on the topic of privacy.

And we understand, or have heard rumors of legislation coming in the next few weeks, and I look forward to that, and working with you on legislation to improve rights of privacy.

As I have stated before, I believe an individual's information is their own personal property. We, as consumers, should know what information is gathered about us, where and how it is stored and protected, and who has access to that stored information. And most importantly, for the context of this hearing, with whom and for what purposes is that information shared?

But the fact of the matter is that information collection, aggregation, and sharing predates the Internet by decades, and yet, most of us don't know the details of who has the information, what information they have about us, and where they obtained it. The most critical point of concern for me is not necessarily the aggregation of this data offline, but when that comparatively limited offline data is combined with more comprehensive data collected online. I believe that that is the most important development, because it will continue to grow in significance, as e-commerce and mobile commerce expand.

The flipside of my concern for privacy and the right to control my information is the recognition that this information sharing is good

for business, and I certainly do feel that I have, or do not feel that I have been harmed because a retail catalog appeared on my mail. Maybe the tenth one in one day, yes, I have been harmed, but. However, we all know that collected information can, in certain contexts, be used by criminals that have, if that information is not respected and protected.

In general, I believe the free market can and should be allowed to solve these types of issues, as consumers become aware and demand certain protections, practices, and control options, industry will respond in order to maintain those vital relationships.

Thankfully, the best actors do take privacy seriously, and they do provide options for consumers to block the sharing of their information for marketing purposes. The problem for Congress is similar to what we face on many issues, and that is how to address the bad actors without overburdening the good by depressing or even eliminating productive and beneficial commercial activity. That is the balance for which we should strive, and the approach that I will continue to support.

I look forward to hearing from our witnesses today, particularly our small business representative. I would like to know exactly what information you collect, with whom you share it, and how you and your partners use that information. I would also like to hear all of your thoughts about how this can be addressed through industry self-regulation, and what, if any steps Congress may need to consider to ensure personal information and the use of that information are adequately protected and treated properly.

Finally, I would like to know your thoughts on how the varying approaches to potential regulation of sharing we have previously discussed in this committee, such as first party, third party approach, or a primary personal approach would impact the world of small business. We have seen, in other contexts, the consequences of acting too quickly without full investigation of potential consequences. In this area that is so important to so many people, I want to make sure that any policy decisions are based upon the fullest information available, and will be fair to all businesses, regardless of their size and corporate structure.

We all want to protect privacy and prevent harm, but Congress should not seek to solve the issue by choosing winners and losers.

Thank you very much, Mr. Chairman, and I thank you, witnesses, for your time and your input today, and yield back the balance of my time.

[The prepared statement of Mr. Radanovich follows:]

Statement of the Honorable George Radanovich
Ranking Member, Subcommittee on Commerce, Trade and Consumer Protection
Hearing on the Collection and Use of Online and Offline Consumer Information
November 19, 2009

Thank you, Mr. Chairman. I am pleased we are holding our second hearing on the topic of privacy. Although we have heard rumors of a legislative proposal in the works, I have yet to see the text and think this hearing will prove insightful if that rumor is true.

As I've stated in similar words before, I believe one's personal information belongs to that person. We as consumers should know what information is gathered about us, where and how it is stored and protected, who has access to that stored information, and – most importantly for the context of this hearing – with whom and for what purposes is that information shared. But the fact of the matter is that information collection, aggregation, and sharing predates the Internet by decades, yet most of us don't know the details of who has the information, what information they have about us, or where they obtained it.

The most critical point of concern for me is not necessarily the aggregation of this data offline, but when that comparatively limited offline data is combined with the more comprehensive data collected online. For me, that's the most important development because it will continue to grow in significance as e-commerce and mobile commerce expand.

The flip side to my concern for privacy and the right to control my information is the recognition that this information-sharing is good for business, and I do not feel I have been harmed because a retail catalog appeared in my mail. But what's good for business can also be good for criminals if that information is not respected and protected.

In general, I believe the free market will solve these types of issues. As consumers become aware and demand certain protections, practices, or control options, industry will respond. Thankfully the best actors do take privacy seriously and do provide options for consumers to block the sharing of their information for marketing purposes. The problem for Congress is similar to any issue we face: the concern is not necessarily in response to the good actors, but rather how to address the bad actors.

I look forward to hearing from our witnesses today, particularly our small business representative. I'd like to know exactly what information you collect; with whom you share it; and how you and your partners use that information. I'd also like to hear your thoughts on what, if any, steps Congress may need to consider to ensure personal information and the use of that information is adequately protected and treated properly. Finally, I'd like to know your thoughts on how the varying approaches to protecting information sharing we've previously discussed in this Committee – such as a first party/third party approach or a primary purpose approach – would impact the world of small business.

We've seen in other contexts the consequences of acting too quickly without full investigation of potential consequences. In this area that is so important to so many people, I want to make sure that any policy decisions are based upon the fullest information available and will be fair to all businesses, regardless of their size or corporate structure. We all want to protect privacy and prevent harm, but Congress should not seek to solve the issue by choosing winners and losers.

Thank you to our witnesses for your time and input today. I yield back, Mr. Chairman.

Mr. RUSH. The chair thanks the gentleman, the vice chair, or the ranking member, rather.

The chair now recognizes the gentleman from Massachusetts, Mr. Markey, for 5 minutes, for the purposes of opening statement.

OPENING STATEMENT OF HON. EDWARD J. MARKEY, A REPRESENTATIVE IN CONGRESS FROM THE COMMONWEALTH OF MASSACHUSETTS

Mr. MARKEY. Thank you, Mr. Chairman, very much, and thank you so much for holding this critically important hearing.

Shakespeare, in Othello, said: "Who steals my purse steals trash. 'tis something, nothing; 'Twas mine, 'tis his, and has been slave to thousands; but he that filches from me my good name robs me of that which not enriches him but makes me poor indeed."

Now, as we were growing up, our doctors, our bankers, the nurses, they were privacy keepers. We knew that our medical record was locked up in that closet with the nurse, with the key to open it up to go in and get the records, and it wasn't going to be shared with the neighborhood. The same thing is true for all of our records.

But we have moved from an era now of privacy keepers to one of privacy peepers, and data mining reapers, who want to turn our information into products. And what is the product? The product is our records, our privacy, our families' history. And as online and wireless merge, it becomes all the more possible to take this world, and to compromise the privacy of Americans.

And so, this really goes to the heart of who we are. We wouldn't let the government do this. We wouldn't let the government gather all this information, or make it a product. So, we have to protect against businesses that think that we are all products, that our families are all products. The members of our families are all products, because this information is invaluable as a product to other people.

But to us, it goes right to the essence of our families and who we are, and what privacy we should have a right to expect. And so, as we are moving forward, we have to create the rules. The new technologies themselves have no personality at all. They are just technologies. They only get their personality as we, we animate them with the values that we want them to serve.

And so, for my part, I think that the old values served us very well, and the new technologies should be animated with those old values. That is the key to this discussion. It is not oh, Congress can't keep up with new technology. Oh, we can keep up with it. We know what is going on. The question is, do we have the insight and the courage to add those old values, so that families aren't compromised by businesses that want to make a product out of people's business.

When we were doing the health IT bill in February, adding that $20 billion, I authored the language that ensured that the information that was now going to be transmitted was indecipherable to unauthorized users. Because yes, we want to get the benefit of new health IT information, because that can help patients, but we don't want that information to now be compromised, as it is taken out of the file and put online. We want the benefits to flow to the pa-

tients, but not for the information to be turned into a product, a profile, that can then have everyone in town or everyone across the country knowing who had anorexia, prostate cancer, breast cancer, in your family.

If you want to tell someone about it, you should be able to do it, but if you don't want to tell anyone about it, that should be your right, too. And there is many people who don't mind people finding out, but there is many others who aren't going to tell anyone else in their family that they have a secret. That should be their right. That shouldn't be a decision made by a business, that is now just widely disseminated because there might be more products that they can help you with, to gain access to. They should ask you if you want to have access to it, then that information can be sent out there.

So, this brave new world is really no different than the discussion that our grandparents and our parents had to have about the privacy they expected, and I think that the same values exist, the technologies should work for families, and they should have the right to say no. They should have the knowledge and information that is being gathered about them. They should have the notice that the information is going to be used for other purposes, other than that which was originally intended, and they should have the right to say no. No, well, I want the benefit of the technology, but I don't want it turned into a product. I don't want my children's, my mother and father's information now as some kind of product that is out there.

So, thank you, Mr. Chairman. We could not have a more important subject. I yield back the balance of my time.

I yield back the balance of my time.

Mr. RUSH. The chair thanks the chairman of the Subcommittee on Energy. Now, the chair recognizes the ranking member of the Subcommittee on Energy, Mr. Stearns, for 5 minutes, for the purposes of opening statement.

OPENING STATEMENT OF HON. CLIFF STEARNS, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF FLORIDA

Mr. STEARNS. Thank you, Mr. Chairman, and let me commend you also, you and Mr. Boucher, for having this hearing. I thank the witnesses for coming. We look forward to your testimony.

We have had, I think, back in June, we had a big discussion on behavioral advertising, and how to broadly examine how companies are using consumer Internet behavior to tailor online advertising, to simply identify the ways this kind of targeted advertising affects the consumer. How does he or she benefit from this, and I think most of the feelings were that the consumer does benefit from this.

So, in a sense, this committee is here to hear more about the subject, but also, with an understanding to do no harm. Only the consumer knows how he or she feels about the information being collected, parties that are doing the collecting, and of course, the purpose for which the information is being collected for.

The question becomes just how much influence and how much regulation should Congress be involved with. I don't think Congress cannot and should not make the decision for the consumer. The consumer should make that decision for themselves.

We, as members of this committee, certainly can play a proactive role in ensuring that consumers have this adequate information, and full range of tools at their disposal, in order to simply make this informed choice, whether it is opt-in or opt-out.

Companies that collect information about consumers in both an offline and online manner obviously had to be good stewards of the information, and should seek to protect that information where it is appropriate. Additionally, all companies, whether they be data brokers, major retail companies, or even small businesses, should operate in a transparent manner and fair manner, when it comes to the information they collect about consumers, or consumers, or how that information is subsequently being used.

The real transparency, I guess, is a question of how robust a disclosure and notice to the consumer is required in their privacy policy. They obviously should be presented in a clear, conspicuous manner, so that the consumer knows, should be indicating what is being collected, the ways the information is being used, and third, the ways the consumer can prevent the collection of the information if they don't want to do it.

This is a very significant challenge. We haven't had many hearings on privacy, and understanding the constitutional issues, as well as understanding the role of the Federal Trade Commission. When I was chairing the Commerce, Trade, and Consumer Protection Committee, I realized that there is, people would have different outlooks on the opt-in and opt-out provision.

And I come to believe that for the most part, that if we get into too much of the weeds here, that we are going to impede the Internet, and make it more difficult for people to collect information, when it is probably not necessary.

In fact, at one time, the Federal Trade Commission and I talked about a Good Housekeeping Seal, that would be provided by private companies, that in a sense, would be a seal of approval, so that people, when they went on a Web site, would realize this already complies with a Good Housekeeping Seal that has been approved by the Federal Trade Commission, so that they would have the confidence right there, without going through the rigmarole of looking at an opt-in and opt-out provision, and reading the detailed fine print in a privacy policy.

The small businesses of this country create all of the jobs, and there is a lot of Internet companies that are starting up, and obviously, we wouldn't want to impede their ability to function. So, this Internet is such a powerful means of communication, putting in a significant privacy policy is very important, and has the great effect of either helping, enhancing, or deterring, shall we say, the purchase of products, the use of it.

So, I think this is a very important hearing, to hear from the people that are most involved, and I look forward to hearing from them, and hearing some of the pitfalls of sort of what we have as a draft bill that Mr. Boucher and Mr. Rush and I, and Mr.—others have put together, and so, we are looking forward to, perhaps, after this hearing, to get this draft bill out, so that we can hear from you folks, to see what you think of it. And then, we can move forward.

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

I yield back the balance of my time.

Mr. RUSH. And the chair recognizes Mr. Green for 2 minutes, for the purposes of opening statement.

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

Mr. GREEN. Thank you, Mr. Chairman, both you and Chairman Boucher, thank you for holding this hearing, to continue our examination of consumer data collection and use, and the security and privacy implications it has.

The issue in discussion, of online versus offline data collection, is an important one, because the distinction has blurred so much over the past decade. The ability to easily aggregate and share information over the Internet has proved tremendous benefits to our society and our economy, and the collection of consumer information can provide tremendous benefits to small and upstart businesses, by allowing them to target customers that have tendencies to purchase individualized products or services.

One problem I hear is these aren't the only uses for this data, and the ability of entities that sell this information to collect such a wide variety of information on individuals is extremely troubling, because it allows bad actors to target vulnerable individuals, based on very specific and granular data, that has been collected across a line of online and offline platforms.

Another problem is that this information creates a personal record that few, if any, consumers know what exactly is contained in it. Consumers have no ability to edit that profile, like they would their credit report, but the records maintained on the databases are unregulated, and often maintained more and wider-ranging information than in a credit report, if the information is not used for products or services that fall under the Fair Credit Reporting Act.

Information about transactions, behaviors, and online, offline, and that occur offline, are also becoming more prevalent in these records that can be purchased from companies that sell this marketing information. Nearly every chain store has some sort of discount or club card to collect information of consumer trends. Records are kept and sold of individuals who enter various sweepstakes through the mail. Social networking sites provide, possibly, the greatest threat, because they contain day to day activity of tens of millions of frequent users.

The aggregate of all of this data can provide a tremendously detailed picture of a person's daily life, interests, habits, and behavior, which that person may never know exists. We have laws that regulate how this information can be used by financial institutions and relating to medical privacy, but outside of these defined areas, this information is largely unregulated, and has the potential to tremendously harm consumers.

And I want to thank the chair of both subcommittees for the hearing today, and continue looking into this issue, and I look forward to our witnesses' testimony.

I yield back the balance of my time.

Mr. RUSH. The chair thanks the gentleman. The chair now recognizes the gentleman from Illinois, Mr. Shimkus, for 2 minutes.

Mr. SHIMKUS. Thank you, Mr. Chairman. I will be brief.

We have free over-the-air radio. We have free over-the-air TV. We have free email. We live in a great country, and one of the reasons why we have free email is the ability for people to put advertising banners on that.

And I am talking about Gmail and Hotmail, and we need to be very, very careful that this great benefit, that millions of Americans take advantage of, does not get hindered, disrupted, or destroyed by aggressive legislation in this area, and I yield back my time.

I yield back the balance of my time.

Mr. RUSH. The chair thanks the gentleman for his brevity. The chair now recognizes the gentleman from Pennsylvania, Mr. Doyle, for 2 minutes.

OPENING STATEMENT OF HON. MICHAEL F. DOYLE, A REPRESENTATIVE IN CONGRESS FROM THE COMMONWEALTH OF PENNSYLVANIA

Mr. DOYLE. Thank you, Mr. Chairman, for holding this hearing today. Trading and selling of personal information began as long ago as 1899. Two brothers created the Retail Credit Company to track the creditworthiness of Atlanta grocery and retail customers. Some people know that company now as Equifax.

Since then, the cost of storing and manipulating information has fallen sharply, and now, organizations capture increasing amounts of data about individual behavior. Consumers hunger for personalization. Products, services, Web sites that cater to them, that causes them to reveal information about themselves.

Ordering off a catalog reveals other information. Using their credit card yields more, and thinking you have to send in that warranty card can reveal almost your entire life to other parties.

But that information probably delivers better products, more targeted services, and a more enjoyable Internet experience. As Alessandro Acquisti of Carnegie Mellon writes: "Is there a combination of economic incentives and technological solutions to privacy issues that is acceptable for the individual and beneficial to society? In other words, is there a sweet spot that satisfies the interests of all parties?"

And then, what are the rules of the road that we need to put in place to make sure that consumers' privacy is protected and that commerce flourishes? That is what I hope to learn more about in today's hearing.

I want to credit the work dozens of dedicated faculty and students, working on consumers' data privacy at Carnegie Mellon University, located in the heart of my district, have done. CMU, the Data Privacy Lab, and CyLab, have all greatly contributed to the academic literature, commercial consciousness, public awareness, and my understanding of this issue.

Thank you, Mr. Chairman, and I yield back.

I yield back the balance of my time.

Mr. RUSH. The chair thanks the gentleman. The chair now recognizes the gentleman from Louisiana, Mr. Scalise, for 2 minutes.

OPENING STATEMENT OF HON. STEVE SCALISE, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF LOUISIANA

Mr. SCALISE. Thank you, Chairman Rush and Boucher. I want to thank you and Ranking Members Radanovich and Stearns for having this hearing on the collection and use of personal information.

I am pleased that both subcommittees are examining this issue. I know that Congress and this committee have held hearings on privacy in the past, but as we all know, consumers' personal information is being collected more and more every day, often without their knowledge, through both online and offline modes of commerce. Whether they are participating in a survey, using Facebook, or even ordering a product over the phone.

Given the importance of information in today's economy, and given how often consumers give out their personal information, there is a genuine cause for concern. Therefore, we must continue to examine ways to ensure consumers don't have their personal information compromised or misused.

As one pointed out in our last joint hearing, many Internet companies are offering the ability to opt-in or opt-out of the company's policies to use or share personal information they collect. But those policies often do not address the collection of the data. The collection and use of personal information can help companies better serve customers, market products to certain consumers, and verify consumers' identity.

But the potential for danger does exist. Personal information could easily be compromised, and there are bad actors that use consumers' personal information in ways that take advantage of the consumer, and in some cases, in ways that are illegal.

Consequently, there are issues that we must address. As we take those into consideration, and debate the best steps moving forward, I hope we proceed carefully when drafting legislation in this area. As I stated at the previous hearing on behavioral advertising, I hope the focus of today's hearing is how we can protect consumers and their personal information, and what steps the industry will take on their own to do that.

I hope today's hearing does not focus on ways government can get more involved in areas of people's lives where it does not belong. For this reason, I believe that if self-regulation is not sufficient, and if any privacy regulatory requirements are needed, they should be targeted, consistent, and not be greater for one business or industry than they are for another. Congress should not pick winners and losers.

I look forward to hearing the comments of our panelists today, particularly on the collection of data through offline methods, and how companies are using this data. I also hope to hear about current security measures that companies have in place, and any they may be planning to implement in the future, to ensure the protection of personal information.

It is important that these committees understand their positions and activities, as well as all of the implications of collecting and using personal information.

Thank you, and I yield back.

I yield back the balance of my time.

Mr. RUSH. The chair thanks the gentleman. The chair now recognizes the gentlelady from California, Mrs. Matsui, for 2 minutes.

OPENING STATEMENT OF HON. DORIS O. MATSUI, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA

Ms. MATSUI. Thank you, Mr. Chairman, and I thank you and Chairman Boucher for calling today's joint hearing. And I applaud your leadership in addressing this important issue. I would like to also thank our panelists for being with us this afternoon.

Today, we will be examining the collection and commercial use of consumer information across the offline, online, and mobile marketplaces. Without their knowledge or approval, consumers' personal information is being collected when they conduct daily activities, such as using the Internet, shopping at the grocery store, or even ordering takeout from their local favorite restaurants, and that is just to name a few.

In today's economy, information is everywhere, and it is to everyone. Unfortunately, it is essentially impossible to protect one's personal information these days, and it is understandable that most Americans simply do not trust that their personal information is properly protected.

Privacy policies and disclosures should be clear and transparent, so consumers can choose what information, if any, they want others to know, instead of inappropriate collection and misuse of that information. Consumers should also understand the scope of the information that is being collected, what it is being used for, the length of time it is being retained, and its security. The more information that consumers have, the better.

Moving forward, we must assure that Americans feel secure that their personal information will not be misused the next time they surf the Internet, shop at a grocery store, or eat carryout from a restaurant. Meaningful privacy safeguards should be in place, while making certain that we do not stifle innovation.

Thank you, again, Mr. Chairman, for holding this important hearing, and I yield back the balance of my time.

I yield back the balance of my time.

Mr. RUSH. The chair thanks the gentlelady. The gentlelady from Tennessee is recognized for 2 minutes.

OPENING STATEMENT OF HON. MARSHA BLACKBURN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TENNESSEE

Mrs. BLACKBURN. Thank you, Mr. Chairman, and welcome to our witnesses. We are glad you are here, and I am pleased that we are having this hearing today.

Nearly everything that we do on the Internet is monitored, and one of the things that we need to do is make certain that there is an understanding of what a level of privacy is, and what those expectations are, and make certain that we put some good rules of the road in place.

At the same time, we don't want to stifle the engines of Internet commerce and e-commerce, that have been an absolutely wonderful economic driver, especially for many small businesses. And in areas

like mine, all the area from Memphis to Nashville, where we have so many small businesses that do depend on those e-commerce formats to make certain that they are profitable.

Now, my constituents in Tennessee have raised with me the issue that there does seem to be an alarming trend, in which ads from some well-known brands are consistently appearing on sites that traffic illegal content, such as pirated movies and music, and these sites are often located outside the U.S., and may be linked to broader criminal enterprises, that clearly have no regard for the privacy of others. They are very concerned about this, and they want to make certain that that is an issue that is addressed, as we move forward in this debate.

They are also concerned about rules, as we look at privacy, something that, about Congress getting in the business of dictating what data is acceptable or unacceptable, and distorting how that travels up and down the pipe.

So, we need to be responsible, looking for responsible solutions that are going to both protect consumers and empower consumers to have control over their data, and allow businesses to continue with their e-commerce format.

So, welcome, look forward to hearing your comments.

I yield back the balance of my time.

Mr. BOUCHER [presiding]. Thank you very much, Ms. Blackburn. The gentleman from Maryland, Mr. Sarbanes, is recognized for 5 minutes.

Mr. SARBANES. I waive. I waive my opening.

I yield back the balance of my time.

Mr. BOUCHER. I am sorry. Mr. Sarbanes, did you waive a statement? OK. The gentleman will have time added to his question period.

The gentleman from California, Mr. McNerney, is recognized for 2 minutes.

Mr. MCNERNEY. Well, thank you. I commend Chairman Rush and Chairman Boucher for convening this fascinating and important hearing.

As technology develops, the opportunity for abuse, I believe, is going to grow exponentially, and consequently, policy does need to keep pace, to ensure that consumers are protected.

A couple of things that I would like to learn this morning, this afternoon. First of all, I would like to get an idea of the scope of the potential problems. How is this data going to be able to be used to affect our lives? And secondly, I would like to understand what makes sense, in terms of how data access and data use can and should be restricted. And I want to thank you all. You represent organizations that collect data and use data, so you are on the frontlines.

And with that I will yield back.

I yield back the balance of my time.

Mr. BOUCHER. Thank you very much. The gentleman from Ohio, Mr. Space, is recognized for two minutes.

OPENING STATEMENT OF HON. ZACHARY T. SPACE, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF OHIO

Mr. SPACE. Thank you, Chairman Boucher. I would like to thank Chairman Rush and Ranking Members Radanovich and Stearns for convening our subcommittees today to discuss online and offline collection and use of consumer information.

I was struck, in reviewing our witnesses' testimony, that there seems to be limitless sources for information on consumers, publicly available data, data volunteered by customers, and data collected from customer-facing businesses. Taken individually, each of these datasets provides a partial picture of a consumer. However, when these datasets are combined, retailers and data brokers can cobble together a fairly complete customer profile.

And I find this fascinating. I certainly understand the benefits that such datasets can provide to businesses, especially small businesses, as highlighted by, and I hope I don't get this wrong, Ms. Bougie. With a name like Space, I can feel your pain. And to the extent that customer profiling can embrace or enhance commerce, I believe such data gathering is an important tool.

However, as outlined by our witnesses, there are also some concerning possibilities about and regarding abuse of this information. It seems like common sense that there should be some protections built in to shield mentally ill citizens, for example, from repeated, unsolicited, targeted marketing.

The bottom line is that consumer datasets, compiled from information gathered online and offline, and the handling of such data, remain largely unregulated. This strikes me as being the Wild West of e-commerce. So that we have some critical interests to consider, and I welcome the continued discussion on this issue.

I look forward to working on this matter with my colleagues, and I yield back. Thank you, Mr. Chairman.

I yield back the balance of my time.

Mr. BOUCHER. Thank you very much, Mr. Space. The gentleman from Connecticut, Mr. Murphy, is recognized for 2 minutes.

OPENING STATEMENT OF HON. CHRISTOPHER S. MURPHY, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CONNECTICUT

Mr. MURPHY. Thank you, Mr. Chairman. Thank you for the hearing, to our chairmen and our ranking members.

Certainly, I think as we spend more time online, this issue of what data is being collected about each of us is increasingly critical. And I think we can all agree that most consumers would prefer to have a clear understanding of what information is being collected, and how it is being used.

But to some degree, I also believe that these consumers, if they think that the data collection is unobtrusive and inoffensive, and if it is being used, I think this point is important, if it is being used to give them information or opportunities that are relevant to them, that are catered to their interests, I think a lot of folks will take lesser offense to that type of data collection. Certainly, this is all predicated on a system that consumers can trust and verify.

Beyond this, I am interested today, and I hope the witnesses might elaborate on this, how the information that we are talking

about today is being used to direct consumers to or advertise on sites that might engage in the pirating of legal content. Because we know there are a vast number of sites available to users whose business model is developed on providing pirated content to individuals, sometimes for a price, and sometimes, because they are supported by ad revenue for free.

In combating piracy, it seems that we should look at how information derived from consumers is then being used to place advertisements, or direct individuals to places where we know illegal activity is occurring.

I hope to explore this issue in greater detail. I look forward to testimony and to listening to the questions. I thank the chairman and yield back.

I yield back the balance of my time.

Mr. BOUCHER. Thank you very much, Mr. Murphy. The gentleman from Georgia, Mr. Barrow, is recognized for 2 minutes.

OPENING STATEMENT OF HON. JOHN BARROW, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF GEORGIA

Mr. BARROW. I thank the chair. I want to welcome all of the witnesses today.

I especially want to welcome Professor Chris Hoofnagle, whom I remember from many, many, many years ago, when I had the privilege of representing him as a county commissioner. It was obvious to me he was going places, then. I just wished I could stick around for the ride.

Mr. Chairman, I am pleased our subcommittees are meeting today to discuss the issue of online and offline data collection, and the commercial use of consumer information for the purpose of delivering targeted advertising.

I have no doubt that sharing consumer information offers benefits to all of us. The benefits pretty much sell themselves, at least, somebody can sell them. It is the costs that I am worried about.

As information brokerage continues to expand, it becomes more important than ever that we draw the line between enhanced data collection methods on the one hand, and unwarranted breach of personal privacy on the other.

In September, this committee was able to mark up H.R. 1319, the Informed Peer-to-Peer User Act, which I co-sponsored with Congresswoman Bono Mack. That bill tackles the privacy and security risks that come with peer-to-peer file sharing programs. I see the work that we are doing here today as a continuation of that effort, to protect personal privacy without discouraging market and technological innovation.

I want to thank Chairmen Rush and Boucher for their leadership in addressing this issue. With that, I yield back the balance of my time.

I yield back the balance of my time.

Mr. BOUCHER. Thank you very much, Mr. Barrow.

Members having had an opportunity, now, to make opening statements, we turn to our panel of witnesses, and I would like to welcome each of you here this afternoon, and thank you for taking the time to share your view on this subject of great interest to all of us here.

Just a brief word of introduction about each of our witnesses. Mr. Chris, excuse me, Hoofnagle is the Director of Information Privacy Programs at the University of California Berkeley School of Law. Mr. George Pappachen is the Chief Privacy Officer at Kantar/WPP. Jennifer Barrett is the Global Privacy and Public Policy Executive at Acxiom. Zoe Strickland is the Vice President and Chief Privacy Officer for Walmart Stores, Incorporated. Michelle Bougie is the Senior Internet Marketing Manager for LearningResources.com, and EducationalInsights.com. Pat Dixon is the Executive Director of the World Privacy Forum.

Without objection, each of your prepared written statements will be made a part of our record of proceedings today, and we would welcome your oral summaries.

And in the interests of time, because we are not sure when we are going to have recorded votes that may command our presence on the floor for an extended period, we would ask that you try to keep your oral summaries to approximately 5 minutes.

So, Professor Hoofnagle, with that admonition, I will be happy to begin with you.

Mr. HOOFNAGLE. Chairmen——

Mr. BOUCHER. Pull that microphone fairly close, and be sure to turn it on.

STATEMENTS OF CHRIS HOOFNAGLE, DIRECTOR, INFORMATION PRIVACY PROGRAMS, UC BERKELEY SCHOOL OF LAW; GEORGE V. PAPPACHEN, CHIEF PRIVACY OFFICER, KANTAR/WWP; JENNIFER T. BARRETT, GLOBAL PRIVACY AND PUBLIC POLICY EXECUTIVE, ACXIOM; ZOE STRICKLAND, VICE PRESIDENT, CHIEF PRIVACY OFFICER, Walmart STORES, INC.; MICHELLE BOUGIE, SENIOR INTERNET MARKETING MANAGER, LEARNINGRESOURCES.COM AND EDUCATIONALINSIGHTS.COM; AND PAM DIXON, EXECUTIVE DIRECTOR, WORLD PRIVACY FORUM

STATEMENT OF CHRIS HOOFNAGLE

Mr. HOOFNAGLE. Thank you. Chairman Boucher and Ranking Members Radanovich and Stearns, and honorable members of the committee, thank you for holding this hearing today on an often overlooked issue in consumer protection.

While we have debated online privacy issues for the past decade, little attention has been focused upon how businesses collect, use, and disseminate information collected in offline contexts, for instance, at stores, at the point of sale, through surveys, sweepstakes, catalog sales, and the like.

I first approached this issue from a civil liberties perspective. About six years ago, I started highlighting the relationships between offline marketing companies and the government. As Mr. Markey noted in his opening statement, he said that Americans would never allow the government to collect so much information about them. However, I found that many government agencies had simply outsourced their information collection activities on citizens by hiring marketing companies. Offline marketing companies had data on almost every American adult, and they had created tech-

niques to analyze the data that could be adopted to law enforcement and intelligence needs.

More recently, my work has focused upon consumer protection in the offline marketplace. For some time, I tried to call attention to the sale of personal information about consumers among companies. I would find data cards, which are offers to sell personal information databases and put them online. These lists included databases that described consumers in pejorative ways, and I would key up my first exhibit.

This is a list of so-called impulsive consumers. It is difficult to read on the screen, but it is included as Appendix 2 in my testimony. The data marketplace has greatly outpaced legislative and regulatory interventions to protect consumer privacy.

For instance, in California, legislators acted quickly to block phone companies from creating a wireless 411 database. This would be a service to look up cell phone numbers. However, in focusing upon phone companies, California legislators missed the mark. Several data companies with no consumer relations whatsoever now market cell phone databases and other databases that list unlisted and private phone numbers.

Appendix 2 of my testimony gives an example of one that is collected through the phone numbers that are given when you order pizza, and this is my second exhibit. This is an information service that claims to get unlisted and cellular telephone numbers by collecting them from pizza delivery companies.

This brings me to a central point of my testimony today. American privacy law allows most offline businesses to sell customer data without giving the consumer notice or an opportunity to object. My public opinion research at UC Berkeley has focused upon whether consumers understand this. The findings are clear. Americans falsely believe that they enjoy a right of confidentiality with most businesses. This explains why they do not ask for privacy policies at the register, or opt out to information collection. They incorrectly assume that privacy law prohibits the use of their personal information. American don't understand that the burden is upon them to object.

The lack of a legal framework that governs information collection and use offline leads to practices that Americans would object to, if they knew about them. I detail two in my written testimony. First, data companies use confidentiality agreements to keep information sharing secret. This means that if an advertiser wants to buy personal information about a group of people, the seller of the data binds the advertiser to confidentiality.

Database companies prohibit their clients from telling customers how data were acquired, what data were acquired, and what categories the consumer has been placed in. This means that if you go to a business and ask how did you get my information, the advertiser is contractually required to say we cannot tell you. This is part of a larger strategy that leaves consumers in the dark about information selling practices.

Second, in the offline context, and increasingly, in the online world, companies are using enhancement. This is the practice of buying additional data about existing consumers. So, for instance,

have you ever been at a store, and have the cashier ask you what your phone number is?

If you share your phone number, that gives that retailer the ability to reverse lookup your name and home address. Some of these problems could be solved with what I call data provenance, the ability to determine from where data was collected, and the rules and context governing its collection.

Since I have just ten seconds left, I would like to thank the committee again for holding this hearing, and I look forward to your questions.

[The prepared statement of Mr. Hoofnagle follows:]

BerkeleyLaw
UNIVERSITY OF CALIFORNIA

University of California, Berkeley
School of Law
396 Simon Hall
Berkeley, CA 94720-7200
1-510-643-0213
1-510-643-2362
http://bclt.berkeley.edu/
choofnagle@law.berkeley.edu

Testimony and Statement for the Record of Chris Jay Hoofnagle, Lecturer in Residence, UC Berkeley Law

Before the House Energy and Commerce Subcommittees on Commerce, Trade, and Consumer Protection and Communications, Technology, and the Internet

Hearing on "Exploring The Offline And Online Collection And Use Of Consumer Information"

November 19, 2009 | 2123 RHOB

Dear Chairmen Rush and Boucher and Ranking Members Radanovich and Stearns,

Thank you for holding this hearing on the offline and online collection and use of consumer information.

It is undeniable that the sale of collection, use, and dissemination of personal information is critical to the success of a wide variety of businesses. Databases of demographic, behavioral, and "psychographic" profiles help companies identify new sales leads, new product offerings, retain customers who are likely to churn, manage risk, and importantly, identify people who are not likely to buy, thus making marketing more efficient. These practices help level the playing field among small and large businesses and can promote competition.

It is also undeniable that these practices have profound privacy and consumer protection implications. While much public attention has been focused upon information practices online, for a century similar practices have occurred offline. In some respects, consumers have more privacy rights in the online context than the offline context.

My testimony focuses upon offline collection and use of personal information. Polls conducted in 2005, 2007, and 2009 show that many Americans falsely believe that practices common in the offline data marketplace are illegal. Furthermore, many data practices are opaque to consumers, and in some circumstances, data brokers use "gag clauses" to keep consumers in the dark. Finally, some businesses use techniques to subtly identity individuals and link data to consumers without their knowledge or consent. These activities make consumers unwitting participants in profiling and contravene norms of transparency and fairness.

1. Consumer Knowledge of Common Offline Data Practices

In 2005, a team led by Professor Joseph Turow of the University of Pennsylvania's Annenberg School for Communication asked a national sample of Americans about common offline and online privacy practices. They found that, "...many adults who use the internet believe incorrectly that laws prevent online and offline stores from selling their personal information."[1] For instance, 48% incorrectly answered false and 16% "don't know," to the statement, "When I subscribe to a magazine, by law that magazine cannot sell my name to another company unless I give it permission."

In fact, magazine publishers and many other companies can and do sell personal information about customers without statutory protections in place to ensure notice, transparency, choice, or accountability. The enormity of this marketplace is difficult to conceive of. One can start to unravel it by visiting http://lists.nextmark.com/. At this website, 60,000 lists of consumer personal information are sold. The sources of data are myriad; they include: public records, phone books, utilities companies, sweepstakes entry forms, magazine and newspaper subscriptions, purchases from infomercials, credit card companies, product warrant cards, and even services like pizza delivery.[2] Many of these lists include highly sensitive personal information, and some describe consumers in a pejorative way.[3]

Jennifer King, my colleague at UC Berkeley, and I were interested in probing whether Californians understood the rules of this marketplace. In 2007, we participated in the Golden Bear Omnibus Survey, a telephone-based survey of a representative sample of California residents conducted by UC Berkeley's Survey Research Center. We asked Californians about default rules for protecting personal information in nine contexts. In six of contexts (pizza delivery, donations to charities, product warranties, product rebates, phone numbers collected at the register, and catalog sales), a majority either didn't know or falsely believed that opt-in rules

---

[1] J Turow, L Feldman & K Meltzer, *Open to Exploitation: America's Shoppers Online and Offline*, ANNENBERG PUBLIC POLICY CENTER 10 (2005), http://repository.upenn.edu/cgi/viewcontent.cgi?article=1035&context=asc_papers. Relevant questions from this survey are included as Appendix I.

[2] See e.g., 3 Pica Investigative Reporter 15, June 2005, available at http://www.pica-association.org/images/ 6-2005.pdf and Appendix II.

[3] See examples included in Appendix II.

protected personal information from being sold to others.[4] Only in two contexts—newspaper and magazine subscriptions and sweepstakes competitions—did our sample of Californians understand that personal information collected by the company could be sold to others.

Further analysis of the data showed that those with high privacy concern were much more likely to correctly answer the questions compared with those with low or mid-level privacy concern. This means that the segments of the American population most knowledgeable about privacy are also most likely to support new privacy laws. Conversely, those with a poorer understanding of the rules are more likely to be satisfied with the status quo.

In 2009, we collaborated with Joseph Turow on a national survey of internet–using adults, to better understand their conception of the privacy landscape. We found that respondents on average answered only 1.5 of 5 online laws and 1.7 of the 4 offline laws correctly because they falsely assumed government regulations prohibited the sale of data.[5]

Perhaps these are not surprising findings. Professor Alan Westin has long found that about half of Americans believe that, "Most businesses handle the personal information they collect about consumers in a proper and confidential way." This suggests that consumers believe that their transactions are confidential; that businesses cannot share details about consumers without informed consent. Confidentiality represents a very high level of information privacy; one that assumes that disclosure harms the data subject even if the confidential fact is not embarrassing. However, consumers rarely enjoy confidentiality guarantees in ordinary transactions.

Understanding the rules of data collection and use is important because current self-regulatory approaches require the consumer to exercise self help to protect privacy. For consumers to exercise a choice, they must know that it is available to them. In many marketplace contexts, however, they believe that the law has already taken a choice, one that guarantees them confidentiality in their transactions.

---

[4] These questions are available in Appendix I. CJ Hoofnagle & J King, *Research Report: What Californians Understand About Privacy Offline*, (2008), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1133075.

[5] Relevant questions are available in Appendix I. Joseph Turow et al., *Americans Reject Tailored Advertising and Three Activities that Enable It*, SSRN ELIBRARY (2009), http://ssrn.com/paper=1478214.

2. Gag Clauses and the Lack of Data Provenance

Recall that Professor Westin has repeatedly found that American consumers believe that businesses handle personal information in a confidential way. In fact, confidentiality is used regularly by data marketing companies. Database companies prohibit their clients from telling consumers how data were acquired, what data were acquired, and what categories the consumer has been placed in. One standard contract of a data broker requires that direct marketing to consumers, "…shall not contain any indication that Client or Client's customers possess any information about the recipient other than name and address…"

Imagine receiving advertising mail for a child or loved one who died,[6] or marketing based upon receiving in vitro treatments that were ultimately ineffective,[7] or targeted advertising based upon a sensitive medical condition.[8] A consumer might ask, "how did I get on this list." Because of these gag clauses, the answer is: "we won't tell you."

---

[6] "…The PRC [Privacy Rights Clearinghouse] has received numerous complaints from individuals who have recently experienced the death of their spouse. They continue to receive unsolicited mail addressed to that individual long after the death, and long after the surviving spouse has notified the mailers to stop sending solicitations. We have also been contacted by parents who have lost a baby due to miscarriage or Sudden Infant Death Syndrome, but who are receiving mail solicitations relevant to the infant years after the death (for example, "Now that your child is two, you will want to delight him with ... xyz."). There is no reason why these grieving individuals must continue to receive unsolicited mail, once they have told the mailers to cease. Yet, such instances are not uncommon in the annals of the PRC hotline." Comments of Beth Givens, Executive Director, Privacy Rights Clearinghouse, before the Federal Trade Commission workshop on The Information Marketplace: Merging and Exchanging Consumer Data, Apr. 30, 2001, available at http://www.privacyrights.org/ar/ftc-info_mktpl.htm.

[7] Milt Freudenheim, *And You Thought a Prescription Was Private - NYTimes.com*, NEW YORK TIMES, August 9, 2009, http://www.nytimes.com/2009/08/09/business/09privacy.html?_r=2&em=&pagewanted=print.

[8] "Addiction Responders – E-mail, Postal, Telephone: Who is struggling with an addiction to gambling, sex, or food? Who can't "just say no" to drugs, alcohol, or tobacco? Millions of American consumers, and Vente has them. Vente's Addiction Responders file has all the data you need to reach those Americans who suffer with addictions." Vente, Addiction Responders - E-mail, Postal, Telephone, available at http://lists.venteinc.com/market;jsessionid=F62EC8004ECF547ECD814EB33907C378?page=research/category&id=5720

These gag clauses prevent transparency and frustrate self help remedies. They further frustrate "data provenance," the ability to determine from where data was collected and the rules and context governing its collection.

Without data provenance, consumers cannot tell what the original source was for personal information sold about them. This leads to several suboptimal outcomes: lack of data provenance obscures the sale of personal information to scammers. Lack of provenance makes it easier to sell lists where consumers are characterized in pejorative ways. Without provenance, consumers who have some desperate need to stop rediscosure of contact information (for instance, stalking victims or public officials) have no effective way of determining the source that is selling the information. A lack of provenance also makes it easier for companies to make strong privacy guarantees to consumers and illegally sell data to third parties.[9] Consumers have no way of avoiding companies that quietly resell personal information, and thus are robbed of the market opportunity to vote with their feet for more privacy-preserving competitors.

3. Enhancement and Data Appends

Through enhancement, a business can "append" data to personal information that the company already has. For instance, if a retailer collects customers' phone numbers at the register, several US companies will "enhance" that information with additional data, such as name and address.

Consider this recent example from a California case:

> Jessica Pineda visited a store in California owned by Williams-Sonoma Stores, Inc. (the Store) and selected an item to purchase. She then went to the cashier to pay for the item with her credit card. The cashier asked for her zip code, but did not tell her the consequences if she declined to provide the information. Believing that she was required to provide her zip code to complete the transaction, Pineda provided the information. The cashier recorded it into the electronic cash register and then completed the transaction. At the end of the transaction, the Store had Pineda's credit card number, name and zip code recorded in its databases.
>
> After acquiring this information, the Store used customized computer software to perform reverse searches from databases that contain millions of names, e-mail addresses, residential telephone numbers and residential addresses, and are indexed in a manner that

[9] See e.g., Daniel J. Solove, The Datran Media Case: Information Privacy Due Diligence, Apr, 11, 2006, http://www.concurringopinions.com/archives/2006/04/the_datran_medi_1.html

> resembles a reverse telephone book. The Store's software then matched Pineda's now-known name, zip code or other personal information with her previously unknown address, thereby giving the Store access to her name and address."[10]

Through these practices, data companies can identify and attach additional personal information to customer profiles. Data brokers claim that enhancement increases efficiency and that it is a convenient way to connect consumers to businesses they frequent. However, users of enhancement assume that the consumer wants this information to be shared. Instead of simply asking the consumer for information, they use techniques unfamiliar to consumers to elicit it.

I believe that this is unfair to consumers. Enhancement generally occurs without notice to consumers. It also interferes with a basic privacy strategy: selective revelation. Consumers attempt to protect their privacy by limiting disclosure of personal information, but when businesses use enhancement, any amount of information shared can obviate selective revelation.

Conclusion

In our 2009 survey, consumers expressed great frustration with the existing privacy landscape. Seventy percent wanted companies to be fined more than $2,500 for information privacy violations. Ninety-two percent wanted a right to delete personal information held by companies. In reality however, consumers have virtually no statutory rights with respect to offline data. This has led to abuses, including the sale of lists to scammers.

Congress should recognize that the sale of personal information about Americans has many benefits for consumers and for commerce. But it should also recognize that these practices must be performed in such a way that respects the consumer. My testimony has revealed several practices in this space that treat the individual as an object. A rights-based framework that promotes transparency and data provenance could address the harms and affronts to dignity resulting from the offline sale of personal information.

---

[10] *Pineda v. Williams-Sonoma Stores Inc.*, Cal. Ct. App., 4th Dist., No. D054355, certified for publication 10/23/09, available at www.courtinfo.ca.gov/opinions/documents/D054355.DOC.

Appendix I

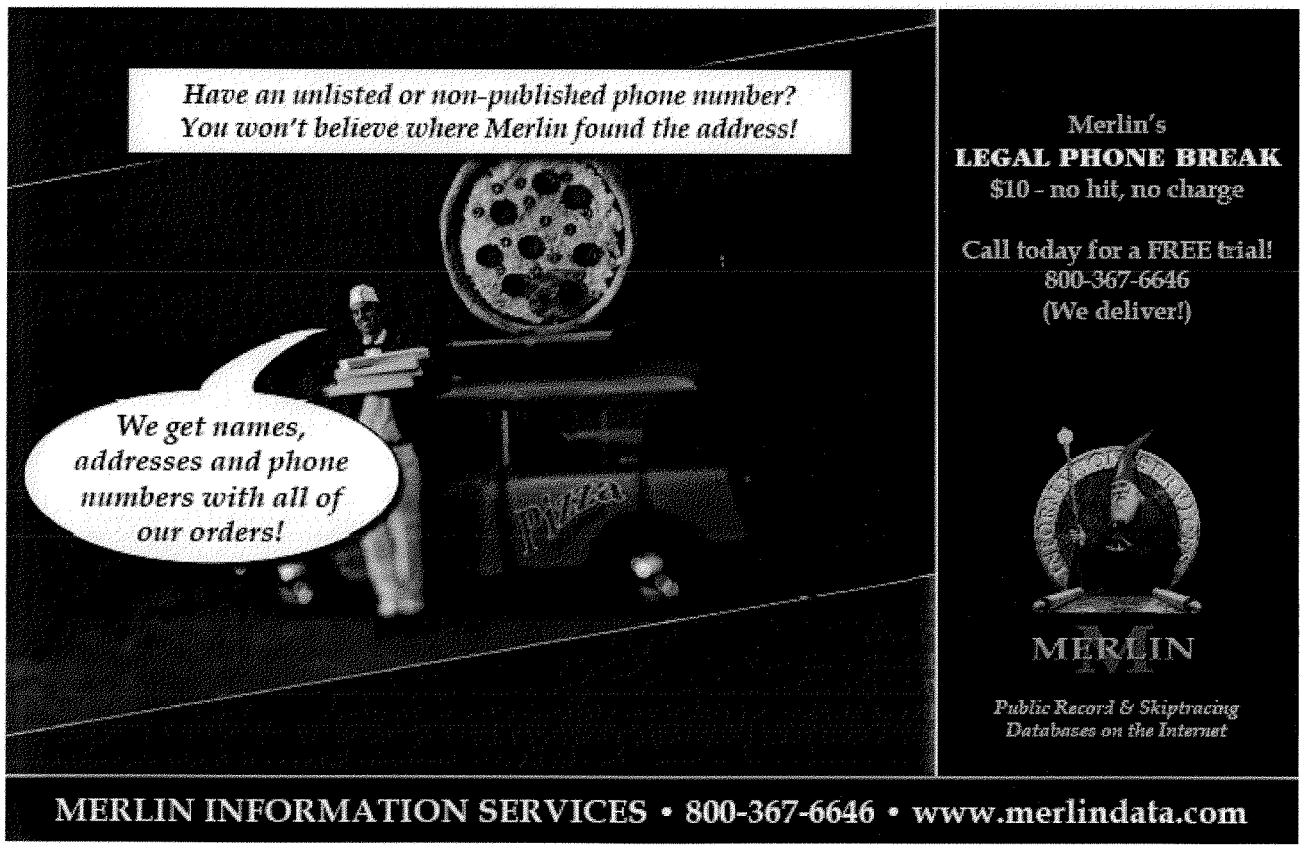
Questions[11],[12]	Year	True	False	DK
When I subscribe to a magazine, by law that magazine cannot sell my name to another company unless I give it permission. (N=1500, national, 2005)	2005	36	**48**	16
When I subscribe to a newspaper or magazine, the publisher is prohibited from selling my address and phone number to other companies, unless I give them explicit permission. (N=309, California only, 2007)	2007	46.6	**50.9**	2.5
When you subscribe to a newspaper or magazine by mail or phone, the publisher is not allowed to sell your address and phone number to other companies without your permission. (N=1000, National, 2009)	2009	36	**49**	15
When I order a pizza to be delivered to my home, the pizza company is prohibited from selling my address and phone number to other companies, unless I give them explicit permission. (N=341, California only, 2007)	2007	54.7	**39.5**	5.8
When you order a pizza by phone for home delivery, the pizza company is not allowed to sell your address and phone number to other companies without your permission. (N=1000, National, 2009)	2009	44	**31**	25
When I give money to charity, by law that charity cannot sell my name to another charity unless I give it permission (N=1500, National, 2005)	2005	47	**28**	25
When I make a donation to a charity, the charity is prohibited from selling my address and phone number to other companies, unless I give them explicit permission. (N=339, California only, 2007)	2007	43.6	**42.4**	13.9
When I enter a sweepstakes contest, the sweepstakes company is prohibited from selling my address or phone number to other companies, unless I give them explicit permission. (N=292, California only, 2007)	2007	42.2	**54.7**	3.1
When you enter a sweepstakes contest, the sweepstakes company is not allowed to sell your address or phone number to other companies without your permission. (N=1000, National, 2009)	2009	28	**57**	15

[11] Questions asked in 2005 have a N of 1500, and derive from J Turow, L Feldman & K Meltzer, *Open to Exploitation: America's Shoppers Online and Offline*, ANNENBERG PUBLIC POLICY CENTER 10 (2005), http://repository.upenn.edu/cgi/viewcontent.cgi?article=1035&context=asc_papers. Questions asked in 2007 derive from CJ Hoofnagle & J King, *Research Report: What Californians Understand About Privacy Offline*, (2008), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1133075. Questions asked in 2009 have a N of 1000 and derive from Joseph Turow et al., *Americans Reject Tailored Advertising and Three Activities that Enable It*, SSRN ELIBRARY (2009), http://ssrn.com/paper=1478214.

[12] The correct answer appears in **bold**.

Appendix I

When I send in a product warranty card, the product manufacturer is prohibited from selling my address or phone number to other companies, unless I give them explicit permission. (N=365, California only, 2007)	2007	50.3	**38.9**	10.8
When I give my phone number to a store cashier, the store is prohibited from selling my address or phone number to other companies, unless I give them explicit permission. (N=333, California only, 2007)	2007	56.9	**38.9**	4.2
When you give your phone number to a store cashier, the store is not allowed to sell your address or phone number to other companies without your permission. (N=1000, National, 2009)	2009	49	**33**	18
When I complete a form for a rebate on a product, the product manufacturer is prohibited from selling my address and phone number to other companies, unless I give them explicit permission. (N=388, California only, 2007)	2007	50.8	**37.2**	12.1
When I order something from a catalog, the catalog company is prohibited from selling my address and phone number to other companies, unless I give them explicit permission. (N=308, California only, 2007)	2007	48.5	**47.9**	3.7
My supermarket is allowed to sell other companies information about what I buy. (N=1500, National, 2005)	2005	**36**	36	28
When I purchase groceries using a loyalty or club card, the grocery store is prohibited from selling my address and phone number to other companies, unless I give them explicit permission. (N=293, California only, 2007)	2007	49.8	42.6	7.6


Have an unlisted or non-published phone number?
You won't believe where Merlin found the address!
We get names, addresses and phone numbers with all of our orders!
Merlin's
LEGAL PHONE BREAK
$10 - no hit, no charge
Call today for a FREE trial!
800-367-6646
(We deliver!)
MERLIN
Public Record & Skiptracing Databases on the Internet
MERLIN INFORMATION SERVICES • 800-367-6646 • www.merlindata.com

AILMENTS, DISEASES & ILLNESS SUFFERERS Mailing List

Here's a brand new database of individuals and households suffering from a wide variety of ailments, diseases, illnesses and medical conditions.

Get More Information | Get a Price Quote

SEGMENTS		COUNTS THROUGH
200,000,000	TOTAL UNIVERSE / BASE RATE	$150.00/M
200,000,000	AILMENT SUFFERERS	$150.00/M
200,000,000	UNLIMITED USE	$300.00/M

DESCRIPTION

Here's a brand new database of individuals and households suffering from a wide variety of ailments, diseases, illnesses and medical conditions. The head of the household or the person with the illness has responded to a questionnaire/survey indicating that someone in the household suffers from an ailment.

Selections include Ailment Type, Age, Income, Ethnicity, Gender, Homeownership, Marital Status, Presence of Children and Telephone.

Permission based E-mail addresses are available. (Rates on request)

Please inquire about counts and pricing.

Select by Ailments: (samples) (from $10/M to $100/M)

Acid Reflux	1,054,900
Acne	1,035,100
Actinic Keratosis	3,161

Preferred Provider

DMA Member

POPULARITY:	***** 98
MARKET:	CONSUMER
MEDIUM:	mail email phone
OPT-IN:	
SOURCE:	LIFESTYLE QUESTIONNAIRE
GEO:	DOMESTIC (US)

SELECTS	
AGE	$10.00/M
ETHNICITY	$25.00/M
GENDER/SEX	$10.00/M
HOME OWNER	$10.00/M
INCOME SELECT	$10.00/M
INDIVIDUAL RESPONDER	$10.00/M
LENGTH OF RESIDENCE	$10.00/M
MAIL RESPONSIVE	$10.00/M
MARITAL STATUS	$10.00/M
PHONE NUMBER	$50.00/M
PRESENCE OF CHILDREN	$10.00/M
SCF	$10.00/M
STATE	$10.00/M
ZIP	$10.00/M

ADDRESSING	
KEY CODING	$5.00/M
DISKETTE	$50.00/F
EMAIL	$50.00/F
P/S LABELS	$15.00/M

HIGHLY CORRELATED LISTS

ADD/ADHD	322,300
Alzheimer's	176,000
Anemia	6,287
Arthritis	10,340,000
Arthritis-Rheumatoid	2,695,000
Asthma	3,663,000
Asthma - Child	111,100
Athletes foot	90,650
Bad Breath	18,978
Bedwetting	367,950
Bladder Control	5,170,000
Blindness /Visual Impairment	7,692,630
Blood Disorder	67,042
Body Odor	7,256
Cancer	633,600
Cancer - Breast	156,200
Cancer-Lung	1,572
Cancer-Other	6,083
Cancer-Prostate	125,400
Canker Sores	1,760,000
Cardiovascular Disease	5,500,000
Cataracts	2,533
Cellulite	23,370

- AILMENTS & HEALTH CONDITIONS
- ACTIVE AILMENTS, DISEASES & CONDITIONS - SUFFERERS & PATIENTS
- MYHEALTHFACTOR - AILMENTS & MEDICATIONS MASTERFILE
- AMERICANS WITH AILMENTS
- MEDICAL AILMENT AND CONDITION POSTAL, EMAIL ADDRESS
- AAA - AILMENT & ILLNESS SUFFERERS
- ABSOLUTE AILMENT SUFFERERS
- SURVEY! AILMENT AND MEDICAL CONDITION SUFFERERS
- CONSUMER LIFETREND RESPONDENTS
- HEALTH AILMENTS RESPONDERS - E-MAIL, POSTAL, TELEPHONE

Cerebral Palsy	1,121
Chronic Bronchitis	1,540,000
Chronic Fatigue Syndrome	13,433
Cold Sores	3,190,000
Colitis	26,950
Constipation	5,720,000
COPD	451,000
Crohn's Disease	42,350
Diabetes (total)	4,985,000
Diabetes - Juvenile	345,400
Diabetes Type 1	328,350
Diabetes Type 2	3,080,000
Dry Eyes	1,650,000
Eczema	440,000
Erectile Dysfunction	932,600
Emphysema	233,200
Endometriosis	49,033
Epilepsy	164,387
Fibromyalgia	6,433
Gastritis/Gastroenteritis	1,038,400
Gum Disease	594,933
Headaches - Frequent	4,950,000
Hearing Difficulty	1,980,000

Heartburn	3,190,000
Hemorrhoids	2,420,000
Hepatitis C - Acquaintance	17,600
Hepatitis C - Self	9,134
Herpes	3,873
High Blood Pressure	122,320,000
High Cholesterol	14,080,000
IBS/Irritable Bowel Syndrome	531,714
Impotence	2,884
Insomnia	9,020,000
Kidney Disease	246,400
Lactose Intolerance	13,090,000
Lupus	3,705
Macular Degeneration	372,900
Menopause	517,000
Menstrual Cramps/PMS	1,127,375
Migraines	7,150,000
Morbid Obesity	1,430,000
Multiple Sclerosis	149,600
Nail Fungus	47,300
Neuropathy/Nerve Pain	332,200
Nosebleeds, Frequent	256,300

Osteoporosis	3,300,000
Pain - Arm and Shoulder	845,478
Pain - Back	3,630,000
Pain - Chronic Pelvic	9,886
Pain - Joint	163,900
Pain - Leg, Hip, Knee, Ankle, Foot	85,923
Pain - Muscle	202,475
Pain -- Total	22,220,000
Pain - Stress & Tension	39,664
Parasites	1,486
Parkinson's Disease	167,200
Physical Handicap	419,100
Poor Leg Circulation	8,533
Prostate - Enlarged	1,002,100
Psoriasis	507,100
Puffy Eyes	14,717
Respiratory Ailments	8,360,000
Rosacea	4,626
Sensitive Skin	1,672,068
Sexual Dysfunction	14,077
Sinusitis	1,323,832
Skin Rash	1,650,000
Snoring	11,220,000
Spinal Disorders	6,699
Spinal Injury	271,504
Sports Injury	639,730
Tooth Decay	18,201
Tumor	4,085
Ulcer	501,600
Urinary Tract Infections	9,225
Vaginal Infections	5,818
Wart	8,671
Wheel Chair	188,100
Yeast Infection	672,007

Sample Mailing Piece Required.

ORDERING INSTRUCTIONS

- To order this list, contact your List Broker and ask for NextMark List ID #102585 or click here to place your request.
- $750.00 MINIMUM PAYMENT
- NET NAME IS NOT ALLOWED
- EXCHANGE IS NOT AVAILABLE
- REUSE IS AVAILABLE ON ORDERS OF 5,000
- PLEASE INQUIRE ABOUT TELEMARKETING

Get More Information | Get a Price Quote

Any questions? View this tutorial or email support@nextmark.com

PULSE TV - INFOMERCIAL BUYERS, IMPULSIVE BUYERS, CREDIT CARD BUYERS Mailing List

Pulse TV (www.pulsetv.com) is an general merchandise retailer that advertises through infomercials. This file is updated monthly with all the new impulsive infomercial credit card buyers. These impulsive infomercial credit card buyers love to buy the newest gadget or product on a impulsive whim. These impulsive infomercial credit card buyers have a very impulsive mindset for buying new products. These impulsive infomercial credit card buyers are constantly watching infomercial TV, checking their mail, and surfing the internet with their credit card in hand ready to buy. Pulse TV's impulsive infomercial credit card buyers are loyal repeat impulsive credit card buyers. As long as there is a new product in front of them that they feel they need or want they have the impulsive nature and the credit card ready to buy. These impulsive infomercial credit card buyers all bought with their credit card and have spent an average of $30 per transaction.

Get More Information | Get a Price Quote

SEGMENTS	COUNTS THROUGH 09/30/2009	
112,920	TOTAL UNIVERSE / BASE RATE	$100.00/M
9,627	SEP 2009	$125.00/M
7,837	AUG 2009	$125.00/M

DESCRIPTION

Pulse TV (www.pulsetv.com) is an general merchandise retailer that advertises through infomercials. This file is updated monthly with all the new impulsive infomercial credit card buyers. These impulsive infomercial credit card buyers love to buy the newest gadget or product on a impulsive whim. These impulsive infomercial credit card buyers have a very impulsive mindset for buying new products. These impulsive infomercial credit card buyers are constantly watching infomercial TV, checking their mail, and surfing the internet with their credit card in hand ready to buy.

Pulse TV's impulsive infomercial credit card buyers are loyal repeat impulsive credit card buyers. As long as there is a new product in front of them that they feel they need or want they have the impulsive nature and the credit card ready to buy. These impulsive infomercial credit card buyers all bought with their credit card and have spent an average of $30 per transaction.

Preferred Provider

MARKET:	CONSUMER
MEDIUM:	mail
SOURCE:	BUYERS
GEO:	DOMESTIC (US)
GENDER:	49.7% FEMALE 47.6% MALE
SPENDING:	$30.00 AVERAGE ORDER

SELECTS	
GENDER/SEX	$10.00/M
GEO/GEOGRAPHICAL	$7.50/M

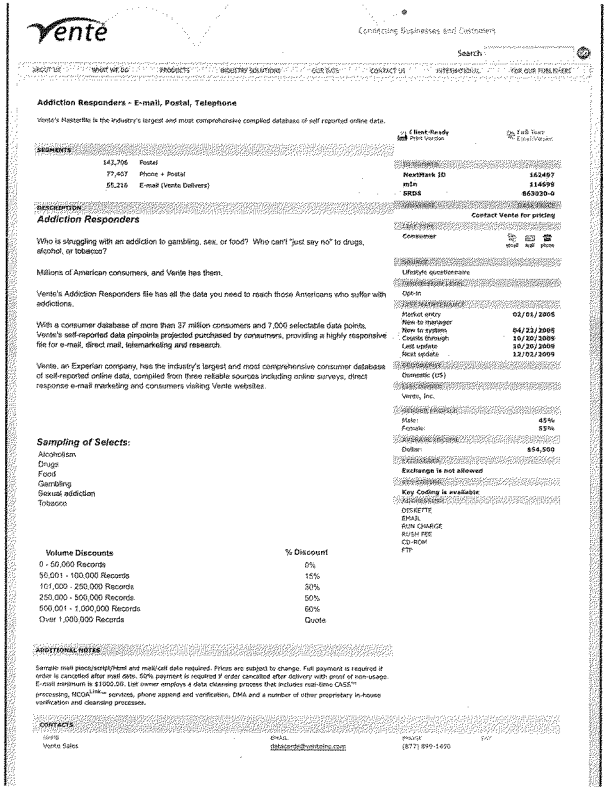
ADDRESSING	
KEY CODING	NOT AVAILABLE
CASS CERT POSTAL PRESORT	NO CHARGE
DMA SUPPRESS	NO CHARGE
EMAIL	$65.00/F

ORDERING INSTRUCTIONS

- To order this list, contact your List Broker and ask for NextMark List ID #271500 or click here to place your request.
- 5,000 NAME MINIMUM ORDER $500.00 MINIMUM PAYMENT
- PLEASE INQUIRE ABOUT NET NAME
- PLEASE INQUIRE ABOUT EXCHANGE
- PLEASE INQUIRE ABOUT REUSE
- TELEMARKETING IS NOT AVAILABLE
- CANCELLATION FEE AT $150.00/F

Get More Information | Get a Price Quote

Any questions? View this tutorial or email support@nextmark.com



Vente

Connecting Businesses and Customers

Search

ABOUT US | WHAT WE DO | PRODUCTS | INDUSTRY SOLUTIONS | OUR DATA | CONTACT US | INTERNATIONAL | FOR OUR PUBLISHERS

Addiction Responders - E-mail, Postal, Telephone

Vente's Masterfile is the industry's largest and most comprehensive compiled database of self-reported online data.

Print Ready Print Version | Full Text E-mail Version

SEGMENTS

142,706	Postal
77,407	Phone + Postal
55,216	E-mail (Vente Delivers)

DESCRIPTION

Addiction Responders

Who is struggling with an addiction to gambling, sex, or food? Who can't "just say no" to drugs, alcohol, or tobacco?

Millions of American consumers, and Vente has them.

Vente's Addiction Responders file has all the data you need to reach those Americans who suffer with addictions.

With a consumer database of more than 37 million consumers and 7,000 selectable data points, Vente's self-reported data pinpoints projected purchases by consumers, providing a highly responsive file for e-mail, direct mail, telemarketing and research.

Vente, an Experian company, has the industry's largest and most comprehensive consumer database of self-reported online data, compiled from three reliable sources including online surveys, direct response e-mail marketing and consumers visiting Vente websites.

Sampling of Selects:

Alcoholism
Drugs
Food
Gambling
Sexual addiction
Tobacco

Volume Discounts	% Discount
0 - 50,000 Records	0%
50,001 - 100,000 Records	15%
101,000 - 250,000 Records	30%
250,000 - 500,000 Records	50%
500,001 - 1,000,000 Records	60%
Over 1,000,000 Records	Quote

ADDITIONAL NOTES

Sample mail piece/script/html and mail/call data required. Prices are subject to change. Full payment is required if order is cancelled after mail date. 50% payment is required if order cancelled after delivery with proof of non-usage. E-mail minimum is $1000.00. List owner employs a data cleansing process that includes real-time CASE[sm] processing, NCOA[Link]sm services, phone append and verification, DMA and a number of other proprietary in-house verification and cleansing processes.

CONTACTS

OWNER	EMAIL	PHONE	FAX
Vente Sales	datasparks@ventelink.com	(877) 899-1499	

NETSOURCE

NextMark ID	162497
mln	114599
SRDS	863030-0

AVAILABLE — Contact Vente for pricing

SELECTS

Consumer — email, mail, phone

SOURCE

Lifestyle questionnaire

TRANSACTION DATE

Opt-in

LIST MAINTENANCE

Market entry	02/01/2005
New to manager	
New to system	04/22/2005
Counts through	10/22/2009
Last update	10/20/2009
Next update	12/02/2009

GEOGRAPHY

Domestic (US)

LIST OWNER

Vente, Inc.

GENDER BREAKOUT

Male:	45%
Female:	55%

AVERAGE ORDER

Dollar: $54,500

EXCHANGES

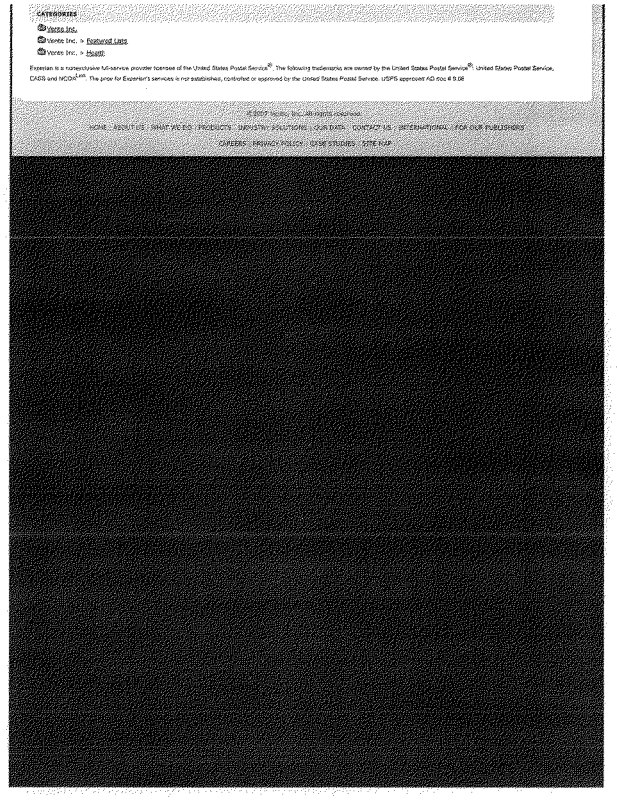
Exchange is not allowed

KEY CODING

Key Coding is available

ACCEPTABLE

DISKETTE
EMAIL
RUN CHARGE
RUSH FEE
CD-ROM
FTP



CATEGORIES

Vente Inc.
Vente Inc. > Featured Lists
Vente Inc. > Health

Experian is a nonexclusive full-service provider licensee of the United States Postal Service®. The following trademarks are owned by the United States Postal Service®: United States Postal Service, CASS and NCOA[Link]. The price for Experian's services is not established, controlled or approved by the United States Postal Service. USPS approved AIS ros # 9.08

HOME | ABOUT US | WHAT WE DO | PRODUCTS | INDUSTRY SOLUTIONS | OUR DATA | CONTACT US | INTERNATIONAL | FOR OUR PUBLISHERS

CAREERS | PRIVACY POLICY | CASE STUDIES | SITE MAP

Mr. BOUCHER. Thank you very much, Mr. Hoofnagle. Mr. Pappachen.

STATEMENT OF GEORGE V. PAPPACHEN

Mr. PAPPACHEN. Chairman Boucher, Chairman Rush, Ranking Members Stearns and Radanovich, and members of the subcommittee, thank you for this opportunity to discuss an issue that is of critical importance to the businesses that I represent.

My name is George Pappachen, and I am the Chief Privacy Officer of Kantar, a division of WPP. As I have been doing in external venues and industry forums on issues of privacy and public policy, I am delighted to represent the interests of both Kantar and WPP here today.

Utilizing information to become as relevant as possible to consumers, and to transform the marketplace of products and services to be responsive to consumer needs, attitudes, and behaviors is at the heart of our business model. As you can appreciate, catering to consumer preferences on a continuous basis is simply not possible without the ability to collect or have access to reliable data and actionable insights.

The dialog taking place today is important, not only for the purpose of awareness and understanding of industry practices, but also, to grant perspective on our shared respect for consumers. Getting it right with regard to our interaction with consumers is an essential element of business success for us. Our brands, and the client brands that we represent, have spent decades building trust with consumers and within the marketplace. Our involvement is really a continuation of that capital investment.

Kantar is one of the world's largest insight, information, and consultancy networks. Covering 80 countries and across the whole spectrum of research and consultancy disciplines, we offer clients insights at each and every point of the consumer or customer cycle.

Our services are employed by a majority of Fortune 500 companies, domestic and foreign governmental entities at all levels, and almost every kind of brand that seeks to communicate to or have a relationship with consumers. We conduct market research, media measurement, which essentially means, for example, how many, knowing, measuring how many people watch TV, versus watch mobile TV, versus watch TV online. And we house consulting and specialty services that run the spectrum from brand value to retail, to healthcare, to government service management.

WWP is the world's leading communications services group. Through its operating companies, the group provides a comprehensive range of advertising and marketing services.

Kantar is a research and consultancy arm of WPP, and houses renowned brands, such as Millward Brown, TNS, Added Value, and Dynamic Logic. Other segments of WPP are creative agencies, such as Ogilvy and JWT, who create advertising, media agencies or other segments, like GroupM, which buy and sell advertising, and our public relations and public affairs firms, many of whom have a strong presence right here in D.C.

Helping clients manage communications has certainly become more challenging in the recent past, due to audiences being more fragmented across the range of media platforms and devices. And

challenging also, because of media convergence, the idea that although people are using different devices to access content, or to communicate, these platforms can be interlinked or overlapped, because of unifying digital language.

Simply put, whereas consumers were confined to a limited number of channels broadcast over a handful of distinct platforms, such as TV, new media has allowed a proliferation of channel choices. Staying ahead of these market shifts, so that we continue to deliver best-in-class services to our clients, who trust us with their investment and advertising and marketing, is a matter of high priority for us.

Consistent with that is our commitment to provide consumers with brand experiences that are relevant and responsible. As noted earlier, Kantar provides market research services, and they use a variety of methods to accomplish this objective. Market research is the voice of the consumer, the user, the citizen, or the donor. As you can surmise, market research fuels a variety of commercial and governmental services.

Researchers use various methods of data collection. Certainly, there are parts of the world where data collection is primarily done offline, via telephone interviews, mall intercept surveys, paper diaries, et cetera. However, in the U.S. in particular, much of our research is now conducted online, online panels, sometimes dedicated to single sectors such as healthcare, web intercept surveys, where consumers are invited in real time, online, to give opinions, online communities, and various other methods are routinely employed.

Some methods utilize cookies or tracking technologies to discern ad exposure, understand site visitation and other metrics. Passive tracking technology has positively impacted market research, in that it allows shorter surveys, and for respondents to not have to observe total recall on all media matters.

It is often said that interactive platforms permit greater customization for the user, and better measurement for the content of service providers. I would agree with that, from an aspirational and inherent capability perspective. While the promise of customization and improvement measurement is real, and progress is encouraging, I believe the medium is still maturing, and still only on its way to fulfill on potential.

Earlier this year, the Federal Trade Commission released its staff report on online behavioral advertising, and this summer, a coalition of industry trade associations, which included the Interactive Advertising Bureau, 4A's and several others, and various businesses, they put forward a self-regulatory framework, to address the issues raised by Congressional and regulatory concerns.

Our companies, like 24/7 Real Media and GroupM, have taken an active role in the coalition work, but we haven't stopped there. We took up the challenge to produce market models, to work out the implementation needs of the proposed self-regulatory scheme. We established a cross-WPP leadership team to develop and test tools, actual tools, which provide enhanced notice and greater transparency about online tracking.

We have sought to collaborate with technology firms and others, who would introduce real solutions for implementing the full elements of the self-regulatory framework.

While behavioral advertising is one way to build a more customized user experience, there are still many other innovations the web enables in this area. Some of them employ designs that don't necessarily require tracking behavior or activity across multiple sites, whereas others do.

It is really the vibrancy of the Internet that allows the variety of the models that we see today. It is terrific.

Mr. BOUCHER. Mr. Pappachen, if you could wrap up. You are well over a minute beyond your time now.

Mr. PAPPACHEN. Traditional and relevant standards, such as personally identifiable information and sensitive data classifications have certainly helped chart the regulatory framework of the online media, and I think has a role to play going forward.

I am of the firm belief that proactive privacy is possible in all areas I have discussed, and that it can be accomplished within a self-regulatory framework.

Building trust with consumers is a primary tenet of any successful business, and we are committed to contributing to a successful formula. I am encouraged by the steps that Members of Congress, and particularly those in these two subcommittees have taken to explore the topic of consumer data collection and use.

I thank the subcommittee for allowing me this time to put forth our position, and I would look forward to staying engaged and active in the ongoing conversation.

[The prepared statement of Mr. Pappachen follows:]

Testimony of George V. Pappachen
Chief Privacy Officer, Kantar, a unit of WPP

Before the Joint Hearing of the Subcommittee on Communications, Technology & the Internet and the Subcommittee on Commerce, Trade & Consumer Protection of the Energy and Commerce Committee of the United States House of Representatives on Exploring Offline and Online Collection and Use of Consumer Information

November 19, 2009

Chairman Boucher, Chairman Rush, Ranking Members Stearns and Radanovich, and Members of the Subcommittees – thank you for this opportunity to discuss an issue that is of critical importance to the businesses that I represent. My name is George Pappachen and I'm the Chief Privacy Officer of Kantar, a division of WPP. As I have been doing in external venues and industry forums on issues of privacy and public policy, I am delighted to represent the interests of both Kantar and WPP here today.

Utilizing information to become as relevant as possible to consumers and to transform the marketplace of products and services to be responsive to consumer needs, attitudes and behaviors is at the heart of the Kantar and WPP business model. As you can appreciate, catering to consumer preferences on a continuous basis is simply not possible without the ability to collect or have access to reliable data and actionable insights.

The dialogue taking place today is important not only for the purpose of awareness and understanding of industry practices but also to grant perspective on our shared respect for consumers. Getting it right with regard to our interaction with consumers – and the points of contact that stand as proxy for their express or implied opinion – is an essential element of business success for us. Our brands and the client brands that we represent have spent decades building trust with consumers and within the marketplace; our involvement today is a continuation of that capital investment.

An overview of our business

Kantar is one of the world's largest insight, information and consultancy networks.[1] By uniting the diverse talents within specialist companies, Kantar is a pre-eminent provider of inspirational and actionable insights for the global business community. Covering 80 countries and across the whole spectrum of research and consultancy disciplines, Kantar offers our clients insights at each and every point of the consumer or customer cycle. Our services are employed by a majority of Fortune 500 companies, domestic and foreign governmental entities at all levels, and almost every kind of brand that seeks to communicate to or have a relationship with consumers.

Kantar is made up of world class businesses that conduct market research (which includes survey, opinion, and social research), media measurement (which informs

[1] *See* www.Kantar.com to get full listing of businesses and additional information about products and services offered. In addition to being leading provider of consumer research, Kantar is listed by Ad Age Daily News (November 17, 2009) as one of the four largest business research providers along with Thomson-Reuters, Bloomberg and Nielsen

about audiences on various platforms), and consulting and specialty services that run the spectrum from brand health to brand value to retail to healthcare to government service measurement. Kantar companies enable brands to craft their communications and gauge the effectiveness and impact of their advertising, their marketing campaigns and various other business initiatives.

WPP is the world's leading communications services group.[2] Through its operating companies, the Group provides a comprehensive range of advertising and marketing services including advertising; media investment management; information, insight and consultancy; public relations and public affairs; branding and identity; healthcare communications; direct, digital, promotion and relationship marketing and specialist communications.

Kantar is the information, insight and consultancy arm of WPP which houses renowned brands such as Millward Brown, TNS and Added Value. Other WPP segments include creative agencies such as Ogilvy and JWT which create advertising, media agencies such as GroupM which buy and sell advertising, and our public relations and public affairs firms, many of whom have a strong presence right here in Washington, DC.

Helping clients manage communications has certainly become more challenging in the recent past due to fragmented audiences and media convergence. Simply put, whereas consumers were confined to a limited number of channels broadcast over a handful of distinct platforms (such as television), new media has allowed a proliferation of channel choices. At the same time, distinct and separate audience platforms isolated by device and location are seeing a convergence toward an interrelated ecosystem. Staying ahead of these market shifts so that we continue to deliver best in class services to our clients, who trust us with their investment in advertising and marketing, is a high priority matter. Consistent with that is our commitment to provide consumers with brand experiences that are relevant and responsible.

Data Collection and Use for Research Purposes

As noted earlier, Kantar companies provide market research services and they use a variety of methods to accomplish this objective. Market research is the voice of the consumer, the user, the citizen or the donor. As you can surmise, market research fuels a variety of commercial and governmental services. Advertisers may be interested in pre-testing their ads before launching or they may be interested in knowing how their ads performed once aired. Others may want to know how their brand is perceived by consumers relative to its competitors in the category, or there may be interest in knowing whether consumers would consider using a new product which is an extension of an existing brand.

A good number of Kantar companies work with governmental agencies around the world. Whether in determining if post mail is reaching its recipients in a timely manner, sometimes in rural areas, or understanding if publicly funded healthcare organizations are delivering the goods, we help ensure that products and services live up to their promise. We have units that work solely on government service measurement. These businesses often have to coordinate across continents,

[2] Ad Age Daily News (November 17, 2009) reports that WPP Group is the world's largest advertising holding company

countries and regions to adopt a standard for measurement that provides a point of comparison across groups, but also allows for differentiation so that local experiences and nuances are not overlooked. Our companies help launch new products that evolve to a more optimized form through research-based trial and error.

Kantar has a specialty media practice with proprietary models to conduct audience measurement so we don't have to stay reliant on paper-based tracking to deliver reliable measurement about what consumers want to watch and what they'll consume or not consume. Dynamic Logic is a unit of Kantar that, among other things, measures the effectiveness of online advertising. They directly ask consumers who have seen the ads they're measuring if they were interesting or meaningful. There was a time when the marketplace thought that the only effective online ads were the ones that recorded a high number of people clicking through them. Dynamic Logic changed that thinking by demonstrating that online ads can have branding impact even if people don't click on them.[3] This learning was instrumental in growing the ad supported internet by helping traditional brand advertisers, such as consumer packaged goods, view the internet as more than the domain of direct response products. We believe that our brands have played a substantial role in growing the ad supported internet that now substantially contributes to this nation's economic value[4] and its social fabric.

To be clear, consumer data we collect for research purposes is not used for direct delivery of advertisement or for solicitation to purchase a product or service. However, the intelligence we produce presents an opportunity for our clients to improve their consumer engagement or customer relationship.[5]

Researchers use various methods of data collection. Certainly, there are parts of the world where data collection is primarily done offline - via telephone interviews, mall intercept surveys, paper diaries, etc. However, in the U.S. in particular, much of research is now conducted online. Online panels (sometimes dedicated to a single sector such as healthcare), web intercept surveys, online communities, and various other methods are routinely employed. Some methods utilize cookies or tracking technologies to discern ad exposure, understand site visitation and other metrics that may either further the goal of a study or preserve data quality. Passive tracking technology has positively impacted market research in that it allows for shorter surveys and for respondents to not have to observe total recall on all media matters.

Notwithstanding the fact that research differs from advertising and the practice of behavioral tracking, which has been an area of focus of consumer privacy discussions, several of our research companies have been pro-active in the area of

---

[3] Dynamic Logic used the term 'beyond the click' to express the brand value of online ads and they continue to produce data that shows the impact of online media which research is regularly presented at this online site, http://www.dynamiclogic.com/na/research/btc/beyond_the_click_dec2004.html

[4] Professors John Deighton and John Quelch of Harvard, in partnership with the IAB and Hamilton Consultants produced study, Economic Value of Ad Supported Internet in June 2009 which is available online at http://www.iab.net/economicvalue and study estimates that the advertising supported Internet accounts for $300 billion of economic activity.

[5] Kantar companies use proprietary panels in combination with real time recruitment and data collection routines to provide aggregated research results to marketers, advertisers, governmental and regulatory bodies, non-profits, and other business entities. Kantar companies do not transfer personal or identifiable information about individual panelists or respondents to their clients

privacy through various initiatives and by working with leading voices such as the Marketing Research Association (MRA) Government Relations Committee. I will later go into some specific examples of some of our initiatives.

Advertising and Data Collection

It is often said that interactive platforms permit greater customization for the user and better measurement for the content or service provider. I would agree with that from an aspirational and inherent capability perspective.

Whereas ad viewing in a traditional TV environment was evaluated either by consumer recall or through journal entries scribbled by a panelist, online ad viewing and engagement does present a new paradigm. While the promise of customization and improved measurement is real and progress is encouraging, I believe the medium is still maturing and still only on its way to fulfilling on potential.

From the attention that behavioral advertising has received, I think it's fair to say that it is viewed as an advanced form of online advertising practice. Earlier this year, the Federal Trade Commission released its staff report on online behavioral advertising[6] and this summer, a coalition of industry trade associations which included the Interactive Advertising Bureau (IAB), 4A's, ANA DMA, BBB, and various businesses, put forward a self-regulatory framework to address the issues raised by congressional and regulatory concerns.[7]

Our companies have taken an active role in the coalition work but we haven't stopped there. We took up the challenge to produce market models to work out the implementation of the proposed self-regulatory scheme. We established a cross-WPP leadership team to work with the Future of Privacy Forum to develop and test consumer touchpoints which provide enhanced notice and greater transparency about online tracking.[8] We have sought to collaborate with technology firms and others who would introduce real solutions for implementing the accountability function and other elements of the self regulatory framework.

While behavioral advertising is one way to build a more customized user experience, there are still many other innovations the web enables in this area. Some of them employ designs that don't necessarily require tracking behavior or activity across multiple sites. Recently, WPP joined with a major media and technology company to launch the Marketing Research Awards Program which funded, for up to $5 million, research studies into better understanding the online environment[9]. In defining the scope of studies that would receive funding, we encouraged submissions that help us

---

[6] In February 2009, FTC released FTC Staff Report titled Self-Regulatory Principles for Online Advertising which is available online at http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf

[7] IAB/ANA/4A's/BBBB/DMA release Comprehensive Privacy Principles for Use and Collection of Behavioral Data in Online Advertising - July 2, 2009 – which is available online at available http://www.iab.net/about_the_iab/recent_press_releases/press_release_archive/press_release/pr-070209

[8] Mediapost article, Can WPP Demystify behavioral targeting?, Wendy Davis, May 20, 2009, which is available online at http://www.mediapost.com/publications/index.cfm?fa=Articles.showArticle&art_aid=106519

[9] More information about the Google & WPP Marketing Research Awards Program is available online at http://research.google.com/university/marketingresearchawards/

better understand consumer attitudes toward data use. Here's an example question we posed to illustrate the type of projects we looked to promote - *How well do consumers understand data collection and targeting and what are measures to improve transparency?*

An MIT project that the program funded this year is titled, "Targeting Ads to Match Cognitive Styles: A Market Test,"[10] which proposed a new design that does not necessarily require tracking across websites but also sought to deliver a more relevant and more customized experience for the end user – an outcome that is desirable for both consumers and brands. The web's capacity for that kind of continual innovation and optimization is unique and should be encouraged.

I cite the program we funded and the MIT study to support this position: It is our hope that the cumulative effect of these multi-faceted efforts produces a better understanding of new media and all of its attendant opportunities and obligations. This is one reason we have taken an active stance in helping move self-regulation from policy design to market-facing model.

Joining Online and Offline

Our active involvement in trade associations and in industry privacy initiatives is to possess a thorough knowledge of consumer issues in all the spheres where our businesses operate. Since online behavioral advertising has been the regulatory focus recently and it is the area where industry has been asked to introduce self-regulation, it follows that this is the area of our greater activism.

The promise of media convergence has the connotation that offline and online would not exist as two distinct worlds in the future, at least in the context of this discussion. A richer experience can result, in some cases, from a responsible joining of online data with offline data that was properly secured. In all such cases, however, the required notice and consent regimes would be expected to be followed.

In most cases of research, the most useful output does not target or identify an individual as a composite of his or her online and offline data. Rather, the objective is to do the opposite - provide insight on a broader, de-identified category of people whose information the marketer can then use along with audience data to improve their communications. A respondent or research subject would only serve as representative of a broader class of people with a matching profile.

Traditional and relevant standards such as personally identifiable information and sensitive data classification have certainly helped chart the regulatory framework for the new medium. However, it is appropriate to consider whether the requisite elements of transparency are properly resident in instances where online and offline data is merged. Consumer expectation is always a key consideration and those expectations can depend in part upon whether proper notice has been made available. And, connected to that is the ability for the consumer to consent or choose among options as to whether and how the data is used or shared.

As a matter of policy, I would hold to the principle that having a proper notice and consent regime in place is only the start – from there, it is incumbent upon the data

[10] Study was designed and conducted by Professor Glen Urban, former Dean of the Sloan School of Management at the Massachusetts Institute of Technology

collector to follow through and only do as it represented it would. The speed at which data moves and the volume of data that can be amassed as a result of digital capabilities is axiomatic. Therefore, it is incumbent on industry to observe that even while we hold firm to the recognized privacy principles that have shaped our policy to date, we would need to ensure that its application to new and evolving data collection and use models does not betray the spirit of those foundational principles.

Pro-active Privacy

I am of the firm belief that pro-active privacy is possible in all the areas I've discussed and that it can be accomplished within a self-regulatory framework. I say this because I've seen it happen. In 2007, I appeared at a Federal Trade Commission workshop[11] and introduced a privacy-enhancing technology that one of our Kantar companies, Safecount (safecount.net),[12] had released. Safecount are experts in online data collection and advanced survey recruitment. Safecount technology identifies consumers who were exposed to a certain ad and then spawns online invitations to them to take surveys so that their answers can be matched against the answers from a group of people who have not seen the ad. The privacy-enhancing technology was Safecount's cookie viewer tool. The cookie viewer enabled the consumer to see, in real time, all the tracking data that Safecount had on them. Additionally, the cookie viewer identified the exact ad from which the Safecount cookie was set and also the place where the ad displayed. This was about promoting transparency on the web – an interested consumer would have full visibility into his or her relationship with Safecount.

As a further step, Safecount, which is in the business of recruiting people to take surveys, also introduced a survey control and choice tool, which would empower consumers to set how frequently they would like to be invited to take a Safecount survey – even not at all. If the cookie viewer was about transparency, the survey choice tool was about delivering control back to consumers so they can actually dictate the terms of engagement. I was pleased to see Google and others come forward since then with similar interfaces that empower consumers to manage the agenda.

GroupM, Ogilvy, Greenfield Consulting, Safecount, Lightspeed Research and 24/7 Real Media are all WPP units that are presently working with the Future of Privacy Forum[13] on the Privacy Icon project. As I mentioned earlier, this project seeks to develop and launch consumer touch-points and experiences that inform of data collection or web tracking. We took the perspective of trying to do for this privacy-enabling project what would be done if we were to launch a market facing brand - and that is develop icons and messages that have potential to develop associations which can then lead to consumer engagement. This project is near conclusion, with the research results planned for release in December.

Earlier this year, a hearing was held by these two subcommittees on behavioral advertising, industry practices and consumer expectations. An annual study that helps industry gauge consumer expectations and awareness of behavioral targeting

[11] FTC's Behavioral Targeting', Session 6, Disclosures to Consumers, on November 2, 2007 and workshop agenda is available online at http://www.ftc.gov/bcp/workshops/ehavioral/agenda.pdf

[12] Safecount's Cookie Viewer tool is at http://www.safecount.net/yourdata.php and its Survey Control tool is at http://www.safecount.net/controlyoursurveyexperience.php

[13] More details about Future of Privacy Forum is located at http://www.futureofprivacy.org/

was cited at the session. The study – "Consumer Attitudes About Behavioral Advertising" – is a collaboration of TNS, a Kantar company, and TRUSTe. I raise this to support the proposition that industry can be pro-active in not only responding to congressional and regulatory overtures but also in keeping a close ear to consumers and their concerns.

Building trust with consumers is a primary tenet of any successful business and we are committed to contributing to a successful formula. I am encouraged by the steps that members of Congress and particularly those in these two subcommittees have taken to explore the topic of consumer data collection and use. I thank the subcommittees for allowing me the time to put forth our position and I look forward to staying engaged and active in the ongoing conversation.

Mr. BOUCHER. Thank you, Mr. Pappachen.

We have two recorded votes pending on the floor of the House. We are going to hear from Ms. Barrett, and then, the subcommittee will briefly recess, while we respond to those votes.

We will pick up when they are concluded.

Ms. Barrett.

Ms. BARRETT. Thank you, Chairman Boucher, Ranking Member Radanovich.

Mr. BOUCHER. And could you pull the microphone very close, please? Thank you.

STATEMENT OF JENNIFER T. BARRETT

Ms. BARRETT. Members of the subcommittee. Thank you the opportunity to share Acxiom's perspective.

First, let me say we are in strong support of appropriate use of consumer information. Protecting privacy has been a priority for us for decades. Use of consumer information to defraud, discriminate, embarrass, or harass consumers is inappropriate, and should be illegal, as it already is in many situations.

However, consumer data make a significant contribution to our Nation's economy, growth, and stability. For 40 years, Acxiom has been a market leader in responsibly providing innovative marketing services and data solutions to help our clients deliver better products and services, smarter, faster, and with less risk.

Marketing services are 70 percent of our revenues, and data solutions are the remaining 30. Our marketing services are specialized computer services that help businesses, nonprofits, and political organizations manage and use their customer information. Although e-commerce has greatly increased the availability of products for consumers, it has also introduced new risks that make a trusted relationship more important, and more difficult.

We help clients accurately identify a particular individual and integrate their information across multiple lines of business and varied points of contact. Our email and mobile message delivery services help our clients respect consumer preferences while complying with various laws like CAN-SPAM.

Our data solutions, on the other hand, provide marketing intelligence and support for identity and risk management decisions. We deliver actionable information not readily available to our clients, to help fill an important gap between knowing what their customers bought and knowing what they like, how they spend their time, and how they feel about certain issues.

Untargeted interactive communications are the junk mail of the digital age, yet this advertising has funded much of what consumers enjoy most about this interactive experience. Consequently, the real winner in the appropriate use of consumer information is the consumer. In the offline world, Acxiom operates in a fully personally identifiable realm, but in the online world, until the consumer chooses to identify themselves to a Web site or an interactive device, Acxiom's solutions, in Acxiom's solutions, the consumer remains anonymous.

We obtain the data we bring to market from several hundred carefully chosen sources. It falls into three general categories. Public records and publicly available data provides names, contact in-

formation, and some demographic information, that come from public directories and other state and local registries. Responses to surveys and questionnaires provide additional demographic, lifestyle, and interest data. Finally, Acxiom acquires some data directly from consumer-facing organizations.

For marketing purposes, consumers are given notice and choice about their data being shared with parties like Acxiom. We use only very general summary data, that would indicate certain lifestyles or interests.

For our identity and risk solutions, the focus is on identifying data, which in some instances, actually comes from heavily regulated industries. It is important to note that Acxiom does not collect online browsing or search activities on consumers.

We have a culture of respecting consumer privacy. Our own guidelines are more restrictive than laws or industry standards. We offer an opt-out from any or all of our marketing solutions, and access and correction in our identity and risk solutions.

Before I close, I want to clear up two common misconceptions. First, Acxiom does not have one big database that contains detailed information about everybody. Instead, we have many databases designed to meet very specific needs or our clients. Second, no marketing information we provide to clients can be used for decisions of credit, insurance underwriting, or employment.

The environment in which data is collected and our clients communicate with their customers has changed a lot in our 40 years. Online is no longer separate and distinct from the offline, mobile, or interactive TV world. Also, privacy is a very contextual issue, and varies by application, while different individuals feel very differently about it.

The committee's greatest challenge is to identify where practices should be regulated by laws, versus what should be covered by interim self-regulation or best practice. Complicating your task is anticipating what changes technology might alter, either in the benefits or the risks.

Similar analysis is taking place across the world, but at present, no one can claim to have developed a truly workable approach. While the committee considers additional regulation, we should be clear about the extent of harm, or market failure it believes has occurred, and look for the least restrictive alternative. Informational hearings help inform all parties where policymakers' concerns lie, and where industry needs more proactive initiatives. However, if privacy laws overreach, everyone suffers, including our economy.

Mr. Chairman, we thank you for the opportunity to be here today, and are available to answer any other questions.

[The prepared statement of Ms. Barrett follows:]

WRITTEN TESTIMONY OF

JENNIFER BARRETT
GLOBAL PRIVACY AND PUBLIC POLICY EXECUTIVE
ACXIOM CORPORATION

BEFORE THE

SUBCOMMITTEE ON COMMERCE, TRADE AND CONSUMER PROTECTION
AND THE
SUBCOMMITTEE ON COMMUNICATIONS, TECHNOLOGY AND THE INTERNET

EXPLORING THE OFFLINE AND ONLINE COLLECTION AND USE OF CONSUMER INFORMATION

NOVEMBER 19, 2009

Written Testimony of Jennifer Barrett
Acxiom Corporation
November 19, 2009

Executive Summary

Acxiom wants to be on the record in strong support of appropriate use of consumer information. Protecting the privacy of individuals has been a focal point for our company since we introduced our first data product in the early 1990s. We believe that the use of consumer information to defraud, discriminate, embarrass or harrass consumers is inappropriate and should be illegal as it already is in many situations. Furthermore, the responsible collection and use of consumer information in the U.S. makes a significant contribution to our nation's economic infrastructure and underpinnings to promote growth and stability.

Privacy is a very contextual issue that varies from application to application and individual to individual. As consumers embrace the use of new technology, almost on a daily basis, the traditional fair information practices that we have historically relied upon are no longer effective, in particular those principles of notice and choice. However, we believe we do not have to sacrifice either the benefits that consumers enjoy from appropriate information use or the benefits that come to businesses, non-profits, political organizations and candidates to protect consumers adequately.

For forty years, Acxiom has been a market leader in responsibly providing innovative marketing services and data solutions. We are proud of our reputation for helping primarily large, but also medium to small businesses, non-profits and political organizations sell better products and services smarter, faster, and at a lower cost. And we do so by applying rules, processes and controls that go far beyond what is required of us by either law or industry self-regulation in order to respect consumer privacy.

Acxiom's business includes both marketing services and data solutions. Our marketing services represent 70 percent of our company's revenue. These specialized computer services assist businesses, non-profits and political organizations in better managing their

customer and supporter information by making marketing decisions possible across multiple lines of business and across multiple touch points with customers.

The remaining 30 percent of our revenues derive from a line of data solutions that provide marketing intelligence and support for identity and risk management decisions. These solutions help businesses, non-profits and political organizations know more about their customers and audiences in a world where the convenience of transacting online has made the relationship with consumers less personal than ever.

In building our data solutions, we use data from public sources, self-reported data from consumers, and data from companies who sell products and services to consumers. Any data included in our data solutions is general in nature and *not specific* to a transaction.

Acxiom has a long-standing tradition and engrained culture of respecting consumer privacy in the development and delivery of our data solutions. We have established our own guidelines that are more restrictive than industry standards. Since 1997, we have posted our privacy policy on our website, and we maintain a Consumer Care Department to handle consumer inquiries. We provide consumers the option to opt out of all our marketing solutions. Consumers can also access the information about them in our identity and risk solutions and correct any inaccuracies they may find.

As business leaders and consumers ourselves, the people of Acxiom are committed to protecting consumer privacy and to increasing consumer understanding of how businesses, non-profits and political organizations use information about consumers – as well as of the benefits that accrue from the flow of such information.

Acxiom believes it is critical that when the Committee considers additional regulation of online data collection and use it should clearly articulate the extent of "harm" or market failure it believes has occurred. To foster innovation, the Committee should evaluate what the least restrictive alternative is in our rapidly evolving technological world and

fully understand the cost of compliance measured against the risk the new regulations would address.

Written Testimony of Jennifer Barrett
Acxiom Corporation
November 19, 2009

Introduction

Chairman Rush, Chairman Boucher, Ranking Member Stearns, Ranking Member Radanovich, and members of the Subcommittees, thank you for the opportunity to participate in this timely hearing and to share Acxiom Corporation's perspective on how the flow of information, both offline and online, is a powerful force in the American economy.

As your Committee continues to explore the issue of privacy, both offline and online, we urge a thoughtful analysis of both the issues and opportunities involved. Privacy is a very contextual issue that varies from application to application. Also, different individuals feel very differently about it. As consumers embrace the use of new technology, almost on a daily basis, the traditional fair information practices that we have historically relied upon are no longer effective, in particular those principles of notice and choice. While this Committee studies these issues, very similar analysis is taking place across the world, but as of this hearing, no country claims to have developed a workable approach.

Acxiom wants to be on the record in strong support of appropriate use of consumer data. Protecting the privacy of individuals has been a focal point for our company since we introduced our first data product in the early 1990s. We believe that the use of consumer information to defraud, discriminate, embarrass or harrass consumers is inappropriate, and should be illegal, as it already is in many situations. Furthermore, the responsible collection and use of information in the U.S. makes a significant contribution to our nation's economic growth and stability by enhancing the variety of goods and services available to consumers, by expanding access to more products, by facilitating special prices and discounts, by providing free content (especially online), and by accelerating the speed, ease and safety with which transactions can be completed.

We believe we do not have to sacrifice either the benefits that consumers enjoy from appropriate information use or the benefits that come to businesses, non-profits, political

organzations and candidates in order to adequately protect consumers. Both of these objectives can be preserved. However, if privacy laws and regulations overreach, the results can be the worst of both worlds: legitimate organizations suffer serious damage, and consumers unintentionally lose many advantages. Ultimately, our economy suffers.

It is our hope that by sharing our story with you – and by separating some of the data myths from reality – we will aid you in determining an appropriate legislative direction.

About Acxiom Corporation

Founded in 1969, Acxiom Corporation has more than forty years of experience in helping our clients turn data into actionable insight while being sensitive to consumer privacy concerns. We are headquartered in Little Rock, Arkansas, with operations throughout the United States, across Europe, and in the Middle East and Asia. Our annual revenues exceed $1 billion. Our company has more than 5,500 employees worldwide: with over 2,400 of them working in Arkansas, over 750 in Illinois, more than 200 in California and Ohio, and over 100 in New York and Tennessee. The remainder are located in the UK, France, Germany, the Netherlands, Portugal, Poland, Saudi Arabia, the United Arab Emirates, China, Australia and New Zealand.

As the global leader in interactive marketing services, advertising and data solutions, Acxiom helps our clients connect with their customers through effective marketing initiatives and sound risk management decisions. Our consultative approach spans multiple industries. For example, Acxiom's clients include:

- 12 of the top 15 credit card issuers
- 7 of the top 10 retail banks
- 9 of the top 10 telecom/media companies
- 9 of the top 10 automotive manufacturers
- 8 of the top 10 property and casualty insurers
- 7 of the top 10 retailers

- 6 of the top 8 brokerage firms
- 3 of the top 5 pharmaceutical manufacturers
- 2 of the top 5 life/health insurance providers
- 2 of the top 3 lodging companies

Acxiom incorporates decades of experience in appropriately using consumer data and analytics, information technology, data integration, and consulting solutions for effective marketing in both the digital and offline world. Our services span the interactive space including email and mobile as well as more traditional direct mail channels. We help our clients establish strong, long-standing relationships with their customers by better understanding what consumers like, what they want and how to communicate most effectively with them.

Interactive Marketing Services and Advertising Solutions

Acxiom's interactive marketing services and advertising solutions, which represent about 70 percent of the company's revenue, include a wide array of leading technologies and specialized computer services. These services help businesses, nonprofit organizations and political parties acquire new customers and supporters as well as improve retention and loyalty over time. We help our clients increase their market share by making the information they have actionable across multiple lines of business and across multiple channels, including the Internet, mobile phones, interactive TV, direct mail, call centers, and even in retail channels.

Accurate management and use of customer information is critical to delivering a positive initial experience for consumers with an organization, maintaining a trusted relationship over time, honoring their preferences about how personal information is used, and improving the bottom line. Although e-commerce has greatly increased the variety and availability of products for consumers, it also has introduced new risks that make

developing a strong, trusted relationship more important and more difficult than ever before.

Acxiom's interactive marketing services and advertising solutions address all these needs. We provide services to accurately identify an individual and integrate the information our client has about this person across multiple lines of business and varied points of contact. We also provide various digital agency services such as our email and mobile delivery capability to help organizations communicate more effectively with consumers and respect their preferences in a manner compliant with all the various laws, such as CAN SPAM, and industry best practices. We also offer website personalization services.

Our marketing services and advertising solutions save our clients millions of dollars by more effectively coordinating their marketing communications and utilizing channels the consumer prefers.

Data Solutions

Acxiom also offers a complementary line of data solutions that represent the remaining 30 percent of our revenues. Our data solutions provide actionable information not readily available to our clients to help fill an important gap between the client and the consumer they wish to engage. Think back a few decades when local shop owners knew their audience well. They were familiar with what their customers bought, how they spent their time, and how they felt about certain issues. Since that time both large and small organizations have worked to achieve a similar level of understanding about their customers' interests and needs. This need for knowledge is nothing new.

However, in the digital age, as consumers shop and interact remotely via the Internet or on their cell phone or PDA, understanding has become much more difficult to accomplish. To put it another way, the Internet initially pushed many organizations back

to the days when all they could do was send mass mailings targeted by geography and census information. This is very ineffective for the organization and results in too many unwanted messages sent to the consumer. Untargeted online communications – email, SMS, pop-up ads, etc. – are the "junk mail" of the digital age.

Our role is to help our clients identify and engage consumers who, based on analysis of the client's own data augmented by Acxiom's data solutions, likely have a need or interest in the client's products, services or causes. While rapidly changing technology, especially online, has largely reshaped the mechanics of how commerce is conducted and relationships are established, the basic strategies in marketing and fundraising remain constant – the operational need to focus a client's outreach efforts on those most likely to have an interest in their product, service or issue.

With Acxiom's data solutions, clients have been able to be successful in the following situations:

- Several distance learning providers and their online vendors looked to us to assure integrity in the education process by using our identity authentication services. Online test takers must answer a series of historical questions to confirm they are the ones actually enrolled in the course.

- An online privacy protection company came to us for a partnership to provide the data and technology for a Protect My Child Registry. The registry helps parents safeguard their children and helps businesses comply with the Children's Online Privacy Protection Act.

- Acxiom gained authorization from the FBI to provide channeling services for companies required to obtain FBI fingerprint-based criminal background checks before hiring for certain jobs. The impact is to uphold commercial integrity among financial institutions and other enterprises facing regulation.

- A political party is using consumer information to determine their best targets for issue-related campaign materials as well as potential donors.

- An online provider looked to us to help them enable consumers to instantly find professional and personal services within their community that have been rated by other consumers.

- Acxiom joined forces with online Yellow Pages directories to provide insight that allows business information to be organized in useful groups for consumers and to include helpful information such as hours of operations, directions and services offered.

- A major managed health insurance company needed help getting its message out to consumers who might need competitively priced individual policies sold direct to the consumer. Acxiom helped them conduct their first direct mail campaign.

- Acxiom was selected by the current administration's open-government initiative to provide the identity card technology that empowers U.S. citizens to register and access various government websites with a single user name and password.

Without supplemental data from Acxiom, the clients in the preceding examples would have been less effective in reducing fraud and communicating with their existing and future customers and supporters. Consequently, the real winner in the appropriate use of information is the consumer.

Developing Acxiom's Data Solutions

Acxiom begins the development of our data solutions by identifying a marketplace need. For example, organizations need to know something about the characteristics of the individuals, households and even devices they intend to contact beyond what they have purchased in the past. 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 age? Other needed information might include whether the household has an interest in certain hobbies, such as cooking or gardening, or sports – do they play tennis, golf or both? Such characteristics are extremely relevant in determining whether a consumer might be interested in certain products, services or issues. Another example would be the need to verify the cell phone number or email address the consumer has provided as valid before allowing that individual to register online so the organization can make contact if necessary.

Once a particular data need by an industry segment has been identified, Acxiom attempts to compile or acquire the relevant information from a variety of sources. The types of sources Acxiom uses are discussed in depth below.

For marketing purposes the information is usually aggregated by household. It is important to emphasize that in all such efforts, any data collected for marketing purposes is general or summarized in nature and ***does not include the details*** **about** an individual purchase or event. In contrast, Acxiom's identity and risk solutions, such as identity verification or fraud detection and prevention services, require data to be maintained at the individual level.

Because different data have different levels of sensitivity to consumers, Acxiom classifies all the data that we include in any data solution, whether for marketing or identity and risk use, as sensitive, restricted or non-sensitive.

Sensitive data is that which could contribute to identity theft. For example, a Social Security number would be considered sensitive data. We do not include any sensitive data elements in our data solutions for marketing purposes, but such information is often a key part of our identity and risk solutions. When sensitive data is involved, special security precautions such as encryption are used to prevent unauthorized access.

Restricted data is that which would be of concern to consumers if it was improperly used or data which has special restrictions placed on it by industry or self-regulation. A cell phone number would be considered restricted data. The inclusion and use of restricted data would follow specifically designated guidelines. For instance, a cell phone number could be used to verify the identity of someone but not to market to that individual without specific consent.

Once the information is collected, Acxiom selects the specific elements needed by the market or application and cleans, integrates and packages the data into a solution that meets the needs of our clients, conforms to all legal requirements and supports any applicable industry self-regulatory guidance. We invest significant time and resources in developing these solutions. A successful data solution provides Acxiom's clients with enough of the right information to solve their specific problem or need.

In the offline world, we operate fully in a personally identifiable realm. As the online world has proliferated, the need for anonymity is greater. Consumers have the choice of whether to identify themselves online. As a result, it is Acxiom's policy that until consumers make the choice to identify themselves personally to a website or other interactive device, the data in Acxiom's solutions remains anonymous.

Acxiom licenses data by the thousands, tens of thousands, or millions of elements or records to qualified businesses, non-profits, political organizations and candidates. We have recently begun to provide some of these solutions, specifically in the identity and risk area, directly to the consumer. We credential and perform a credit check on all

prospective clients. Once we are satisfied with our clients' qualifications and the need for the specific data solution, we require them to sign a contract that binds their use of the information acquired from us for specifically articulated purposes. Acxiom and our clients typically enter into long-term contracts – one, three, five or even more years – for use of a particular data solution.

Acxiom's Data Solutions

Our offline and online data solutions provide needed intelligence for an organization's marketing, identity and risk decisions.

In the area of marketing, Acxiom offers a number of solutions: (1) enhancement of our clients' own customer file with Acxiom data so the client can better understand and respond to its customers' wants, needs and expectations, (2) lists providing access to individuals and businesses for contacting prospective customers, (3) targeted online advertising using a subset of our offline enhancement data, and (4) suppression solutions that allow a client to comply with legislative and self-regulatory guidelines.

In the area of identity and risk solutions, Acxiom also offers several services: (1) employee and tenant background screening services to help employers and landlords gain confidence in a prospective applicant, (2) identity verification and authentication solutions that give an organization confidence it is dealing with a legitimate individual, and (3) our investigate solutions that help organizations locate individuals, assets and principles to resolve delinquent accounts and suspicious activities.

Each of these solutions and the privacy protections that Acxiom has developed to assure the appropriate use of information is discussed in more detail below.

Enhancement Solutions

Acxiom offers businesses, non-profits, political organizations and candidates access to the largest database available of timely demographic, lifestyle and interest data which can be used to enrich their customer or supporter file to better understand their customers' and supporters' desires, needs and changing life-stages. Demographic data includes such elements as the makeup of the household – single, married, and with or without children. Lifestyle data might include such characteristics as lives in an upper income neighborhood, owns a house, or is retired. Interest data would identify a passion for cooking, golf, music or travel.

The client specifies the desired demographic, lifestyle or interest data elements through a menu-oriented approach. This data is then added to our client's already-existing customer or supporter file. It is important to understand the data is general in nature. We do not provide details about specific transactions. Acxiom's enhancement data may be used either offline or online by our clients for marketing and fundraising purposes.

First, enhancement data is used to better understand the interests and needs of current customers, supporters and constitutents. Second, enhancement data is analyzed to identify the best market segments for up-selling or cross-selling purposes. Finally, demographic, lifestyle and interest data helps identify characteristics common in an organization's best customers or supporters to target similarly situated prospects who may be more likely to have an interest or need for certain products or causes.

To make it easier for clients to use the broad types of data Acxiom offers, we have also segmented the entire U.S. population into a series of life stage clusters that can be used to differentiate, for example, young singles from retired couples. Our life stage clusters allow our smaller clients to take advantage of the techniques used by some of the most sophisticated marketers in the world.

We license enhancement data to qualified businesses, non-profits, political organizations and political candidates through a menu-oriented approach. Clients license only the data needed for a particular market or campaign. In many cases, we have pre-packaged data groups to meet common or recurring needs for specific industries.

List Solutions

Our database of more than 95 percent of U.S. households includes contact data as well as demographic, lifestyle and interest characteristics and provides a comprehensive source from which businesses, non-profits, political organizations and candidates can prospect for new customers and supporters. In addition Acxiom's land line telephone directories power most of the yellow and white page search engines on the Internet.

Prospect lists enable businesses to take the experience they have with their best customers and use that knowledge to identify likely households of potential new customers and constituents. Acxiom sells prospect lists to businesses, not-for-profits, political parties and candidates on a one-time use or multi-use basis.

Targeted Online Advertising

With more and more consumers embracing e-commerce, Acxiom has deployed a small subset of our enhancement data including our life stage clusters for online advertising and personalization of websites. Acxiom offers several ways to target messages both personally and anonymously online, via email and mobile. Clients can reach out anonymously to browsers who have shopped at their website, but not bought, with offers to encourage them to return and buy. Clients can use Acxiom's lifestyle clusters to anonymously target display ads to specific audiences on a wide variety of ad-supported websites.

Respecting Privacy in Acxiom's Enhancement, List and Targeted Advertising Solutions

In all our enhancement, list and targeted advertising solutions, Acxiom respects a consumer's choice to remain anonymous. For example, we respect decisions not to publish land line or cell phone numbers. The names and numbers we include in our widely used land line directories are derived only from those consumers who have elected to have their number made publicly available by their local telephone carrier.

All the demographic, lifestyle and interest information is collected from either publicly available sources or from businesses that inform consumers their data will be shared with third parties like Acxiom for marketing purposes. Moreover, consumers can contact us in writing, through our website or via our toll-free Consumer Hotline to opt out of some or all of these products. For instance, a consumer can specify that we not make a phone number available in a Web directory even if it's published in the local printed telephone book. Consumers may also opt out from our targeted online advertising solution but remain part of other marketing offerings.

Suppression Solutions

Acxiom offers our clients one stop to identify individuals who should be suppressed from various marketing campaigns. Our solution includes the FTC National and State Do-Not-Call Registries, identification of wireless phones requiring special consent, the DMA Commitment to Consumer Choice Preference lists, and proprietary underage and deceased suppression services.

Background Screening Services

Our background screening services provide employers and landlords with confidence in a prospective applicant. This service is regulated by the Fair Credit Reporting Act and accordingly requires the permission of the consumer before a background check can be

initiated. We offer these services with the most current information possible by providing a report generated in-person/real-time which includes, but is not limited to, a criminal record check, a credit report and driving record. These services, in combination with others such as drug testing, employment, education and professional license verification, help businesses and non-profits reduce turnover and shrinkage, decrease training costs and increase productivity while protecting the integrity of the companies using them. Organizations can't afford to take unnecessary risks in today's environment relative to employees or renters.

Consumers may also go online to Acxiom.com and order a criminal records report on themselves for a reasonable fee.

Identity Verification and Authentication Solutions

Acxiom's identity verification solutions offer real-time consumer verification that enables the confirmation of identifying information to reduce fraud losses and maintain regulatory compliance. This solution proactively verifies a potential customer's identity in real-time by comparing the data supplied by the consumer against hundreds of public and non-public proprietary sources.

Public record data is obtained from federal, state or governmental records that are open for public inspection. Publicly available data is accessible to the general public from non-governmental sources such as telephone directories, classified ads, newspaper reports, publications or other forms of information both offline and online. The non-public proprietary data is acquired for specific permissible use in a particular industry.

The verification produces a probability score that indicates Acxiom's confidence that the information provided by the consumer is accurate and belongs to a real individual. When the confidence level is not high enough, Acxiom can go one step further and generate questions to pose to the individual to either raise or lower the score.

Investigative Solutions

The pressure on law enforcement agencies to protect Americans from internal and external threats has never been greater. As the U.S. population grows more diverse and mobile, accurate and up-to-date information becomes critical. Even industries such as healthcare and utilities are affected. Acxiom provides an investigative tool created for select, authorized agencies and departments to help accelerate case closures. It can be customized to give access to billions of records cross-referenced from hundreds of data sources, all in a single inquiry that is reliable, easy to use, and sensitive to consumer privacy.

Acxiom also offers an online tool for locating and contacting debtors. It provides accurate information for locating someone who is delinquent and gives information about the property they own.

Sources for Acxiom's Data Solutions

The data we acquire to build our various data solutions is obtained from three general types of sources – public data, self-reported data, and summarized customer data from consumer-facing businesses. Acxiom compiles or acquires this data from several hundred carefully selected and screened sources with whom we have cultivated long-term contractual relationships.

> *Public Data*: Public records and publicly available data are the foundation of Acxiom's data solutions. The types of data that Acxiom acquires or compiles include: white and yellow page telephone directories and other types of publicly available directories, property records, and other state and county public records. This data provides the basic names, addresses and some of the general demographic information, such as home ownership, profession and, in some instances, the age of members of a household. We may acquire and compile this

data from various publicly available websites such as the Florida Department of Business and Professional Registration or the U.S. State Department Terrorist Exclusion List. In some instances use of this data is heavily regulated by federal and state laws such as the Driver's Privacy Protection Act.

Self-Reported Data: Surveys and questionnaires are an additional source for demographic data and provide much of the lifestyle and interest data we compile or acquire. Consumers are asked to voluntarily complete surveys, more often online today, from a variety of companies. In these cases, the consumer is provided the opportunity to opt out of any further use of the data beyond that of the company conducting the survey.

Data from Organizations with Consumers as Customers: Acxiom acquires some data directly from companies who sell products and services to consumers. For marketing purposes, we ensure that consumers have received an opportunity to opt out to prevent their data from being shared with a third party such as Acxiom. Also, we only use very general summary data that indicates possible lifestyle or interest intelligence. We never use detailed transaction data. For example, knowing that a household subscribes to a golf magazine would indicate an interest in golf, just as knowing a household ordered that subscription from a website would indicate the household shops online. For our identity and risk solutions, the focus is on identifying data, and in some instances the source of this data is from a heavily regulated industry such as financial services.

It is important to note that Acxiom does not collect or acquire online browsing or search activity on consumers.

In some cases, Acxiom compiles data directly from the source, such as telephone directories and some consumer surveys. In other cases, Acxiom either acquires this data from other reputable data providers who perform the original compilation, or we acquire

the data directly from the business that has the relationship with the consumer. Acxiom screens all data providers and businesses from which we receive data to assure the data has been legally obtained and is appropriate for the intended use.

It should be understood that while Acxiom has hundreds of potential data elements about a household, the information on any one individual or 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 land line or cell number of a household. We may or may not have property data. We may have some lifestyle or interest data but rarely have all that would apply to the household. Our goal as a data provider is to provide sufficient coverage of a data element to meet the market needs for that particular intelligence.

Respecting Consumer Privacy

Acxiom has a long-standing tradition and engrained culture of respecting consumer privacy in the development and delivery of our data solutions. I have been employed by the company for 35 years and have been responsible for privacy oversight since 1990. Privacy has been my full-time job since the mid-1990s.

Since Acxiom does not have a direct relationship with individual consumers, we do not routinely have direct contact with the individuals even though we hold a lot of data about them. Therefore, we ask our clients to refer to us any individual consumers who may inquire about the source of the data they have obtained from us.

We have posted our privacy policy on our website since 1997, before it was an established and common practice. Acxiom maintains a Consumer Care Department to handle consumer inquiries. We also allow consumers to contact us in writing, through our website or via our toll-free Consumer Hotline to opt out of our marketing products and to access and correct any errors in our identity and risk solutions.

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 Mobile Marketing Association, and the Internet Advertising Bureau. We also hold a TrustE seal. Acxiom is also an active member of the Coalition for Sensible Public Record Access. We have applied for and are in the final stages of being certified as an NAI member. These guidelines include posting a notice that describes what data we collect, how we use it, to whom we sell it, and what choices consumer have about the use of that data.

We believe that consumers should be educated about how businesses use personal information. To that end, we publish a booklet titled "Protecting Your Privacy in the Information Age – *What every consumer should know about the use of individual information.*" available upon written, email or phone request. It is also posted online at http://www.acxiom.com/SiteCollectionDocuments/Resources/Brochures/Protecting_Privacy_Booklet.pdf.

Acxiom takes its responsibility toward protecting consumer information seriously. Beyond the industry-accepted guidelines we follow, we have also established our own guidelines that are more restrictive than industry standards. These include such practices as classifying each data element or combination as either sensitive, restricted or non-sensitive as described earlier. For example, we do not provide Social Security numbers or other personally identifiable information about children in any of our marketing products. Moreover, in compiling information from public records we capture only the specific data required to meet our clients' needs, discarding any remaining data from the source. These voluntary information practices are internally and externally audited on a regular basis.

Myths about Information Providers

Now that you have a better picture of what we do, I believe it is also important to point out what Acxiom *does not* do. Over the years, a number of myths have developed about data brokers that require clarification where Acxiom is concerned. These include:

- 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 business needs of our clients – entities that are carefully screened and with whom we have legally enforceable contractual commitments.

- With the exception of our background screening solution, which is regulated under the Fair Credit Reporting Act, the information we provide to clients *cannot be used*, according to existing law, for decisions of creditworthiness, insurance underwriting or employment. These activities are regulated by the Fair Credit Reporting Act, and such uses are prohibited under our contracts.

- Acxiom *does not* develop for marketing purposes any data solutions that contain sensitive information. We define sensitive information as personal information that could contribute to identity theft as well as personally identifiable information about children.

- 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 websites they visited. All purchase information we provide is general and not specific to an individual transaction.

Challenges in an Interactive World

While our clients' objectives have not changed much in the 40 years we have been in business, the environment in which data is collected and in which our clients

communicate with their customers and supporters has changed dramatically. Offline continues its convergence with online, mobile and interactive TV. Online no longer stands alone as separate and distinct from offline or from other interactive media.

The greatest challenge this Committee faces is to identify what practices should be regulated by law versus what should be allowed to mature and be covered by self-regulation or best practice. Further complicating your task is anticipating what changes in technology might alter either the benefits or risks to consumers. As this Committee has seen in just the last year, technology is moving extremely fast, including privacy-enhancing technologies. We don't want to stifle that innovation.

Acxiom believes it is critical that when the Committee considers additional regulation of online data collection and use, they should be clear about the extent of "harm" or market failure they believe has occurred. The committee should also evaluate what the least restrictive alternative would be in this rapidly evolving technological world and understand the cost of compliance against the risk it is addressing.

Informational hearings such as this one and others the Committee has held in recent years have been very helpful in informing all parties about where the concerns of policy makers lie and where proactive initiatives are needed by industry.

Acxiom understands its responsibility to assure that the information we collect and bring to market provides value to both consumers and our clients. We also consider the risks associated with the collection and use of all data we include in our solutions and take steps to mitigate or eliminate these.

We ask this Committee to do the same – consider the value information brings to consumers and businesses, non-profits and political organizations as it considers regulations related to the online space.

* * *

Chairmen and Ranking Members, on behalf of our more than 5,500 associates, Acxiom appreciates the opportunity to appear today to share with the Subcommittees an overview of our business. We also wish to thank the members of the full Committee 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 Committee may request.

Mr. BOUCHER. Thank you very much, Ms. Barrett. We are going to stand in recess for what will approximately be a half-hour. It may be a bit shorter than that, depending on how quickly the vote goes.

So, stay close, don't venture far, and as soon as we return, we will pick up our hearing.

[Whereupon, at 1:23 p.m., the subcommittee recessed, to reconvene at 1:58 p.m.]

Mr. BOUCHER. The committee will reconvene, and thank you for your patience during our absence.

We continue, with testimony from our expert panel this afternoon, and we are pleased to hear from Ms. Strickland.

STATEMENT OF ZOE STRICKLAND

Ms. STRICKLAND. Good afternoon. Thank you, Chairman Rush. And thank you for inviting Walmart to participate in today's hearing on online and offline privacy.

My name is Zoe Strickland, and I am Walmart's Chief Privacy Officer. For us, good privacy is good business. As the largest retailer and private employer in the U.S., with approximately 140 million customers shopping in our U.S. stores every week, Walmart considers an array of privacy issues on a daily basis.

Unlike companies that interact with customers or other businesses primarily online, Walmart approaches privacy from a very broad perspective. Walmart operations cover almost every conceivable privacy topic, channel, and geographical region.

Given the depth and breadth of Walmart's understanding of consumer privacy issues, we appreciate the committee including Walmart in today's discussion, and would encourage you to engage other similarly situated companies. It is imperative that as privacy rules are developed, legislators take the time to fully understand the impact to consumers that have both online and offline relationships with companies.

Walmart supports a principle-based approach to privacy, rather than a focus on one particular technology or activity. As an example of a principle-based approach, this summer, we updated our customer privacy policy for Walmart operations. The updated policy is based on the Fair Information Practice Principles, as well as industry standards and global guidelines.

Our goal was to make it transparent, meet best practices, and to be integrated across all business units. To further increase transparency, we included a summary notice that links through to the detailed policy. The new privacy policy provides customers more control over their data. Some examples are creating a preference center that allows customers to tell us directly their preferences regarding direct marketing and data sharing for marketing purposes, establishing a stricter standard for data uses customers typically consider more sensitive, Walmart uses opt-in for telemarketing and data sharing, providing additional or enhanced opt-out mechanisms, such as for email ratings and online behavioral advertising, giving customers greater access to their own information, and finally, providing more options to submit questions and concerns.

This initiative gave us further insight into how to focus on underlying privacy principles, and then, to operationalize them. With

regard to online behavioral advertising, Walmart provides clear notices and opt-outs, consistent with the FTC self-regulatory principles, as well as industry best practices.

Equally important, in our view, we integrated our approach into our larger view of privacy in both the online and offline worlds. When and how is it appropriate to give notice? When and how should consumer choice be offered?

We do believe notice and choice are still central privacy protections, even if further protections are warranted. We think our experiences with the use of electronic product code technology, EPC, is a useful example that demonstrates how a broader, principle-based approach is appropriate and needed.

At the simplest level, EPC is a next generation barcode. Currently, EPC is primarily used to track certain cases and pallets in the supply chain. When EPC may be offered on individual products on the sales floor, future, potential customer benefits are real and direct. Examples include receipt-less returns, product authenticity, traceability, and food and product safety.

Even though EPC tags in retail contain no personal data, we are building in privacy protections. As a cornerstone of EPC development, Walmart is designing its use to enable choice. EPC tags will be easily removable from the product or its packaging, such as by placing it on the price tag. If EPC tags used by the retail industry are ever embedded, we will offer a mechanism to disable the tag. We believe that choice is absolutely the right model for this technology.

Some, perhaps most consumers will appreciate its benefits. Some will not, but ultimately, consumers should be able to choose which they prefer.

A challenge, of course, is how to provide appropriate notice. This covers both how consumers know this technology is in operation, and also know what this technology actually means. A variety of methods and channels are possible, including notices on products themselves, notices on or in facilities, and Web site information. You could see how a debate that focuses solely on notices provided on Web sites, like pop-ups, would miss the boat for this technology.

In conclusion, Walmart interacts with consumers frequently, and in every conceivable way. A uniform, or at least consistent privacy framework, that includes standards such as consumer choice is effective for both consumers and businesses.

A privacy regime based on a set of core principles will be sufficiently flexible to be applied in multiple contexts. Consumers deserve to know what to expect with regard to how their information is being collected and used, where they may obtain further details if they desire, and how they can make appropriate choices regarding the use of their data or technology.

Thank you again for the opportunity to testify today. We look forward to continuing to work with you, and I am glad to answer any questions.

[The prepared statement of Ms. Strickland follows:]

Walmart

Hearing on Exploring the Online and Offline Collection and Use of Consumer Information

Testimony of Zoe Strickland, Vice President, Chief Privacy Officer
Wal-Mart Stores, Inc.

Before **the Subcommittee on Communications, Technology and the Internet and the Subcommittee on Commerce, Trade and Consumer Protection** of the Energy and Commerce Committee of the United States House of Representatives

November 19, 2009

I. Introduction

Chairman Rush, Ranking Member Radanovich, and Chairman Boucher and Ranking Member Stearns, thank you for inviting Walmart to participate in today's hearing on online and offline privacy. My name is Zoë Strickland, and I serve as Walmart's Vice-President and Chief Privacy Officer. My role at Walmart provides me with a broad perspective on a range of privacy issues relevant to today's discussion. I appreciate the opportunity to contribute and am honored to offer input that may help inform your consideration of these important policy issues.

II. Walmart's Role

As the largest retailer and private employer in the U.S., with approximately 1.4 million employees and 140 million customers coming through our U.S. stores every week, Walmart considers an array of privacy issues on a daily basis. Unlike companies that interact

with their customers – or other businesses – primarily online, Walmart approaches privacy from a very broad perspective. Walmart operations cover almost every conceivable privacy topic, channel, and geographical region. Walmart operations include:

- Operating as a "brick and mortar" retailer, with over 3500 outlets domestically.
- Operating as a leading online merchant through walmart.com.
- Operating over 600 Sam's Clubs domestically, which offer a membership model with its customers.
- Conducting extensive global operations throughout the world.
- Communicating with our customers across multiple channels, including through email, postal mail, mobile devices, websites, and our stores.
- Collecting and merging data through numerous sources, including customers themselves, third party sources, and technology like websites.
- Providing a wide variety of products and services. Some of these are regulated more than others regarding privacy or personal data. Examples include health services, some covered by HIPAA and some not (like personal health records); financial products and services governed by the Gramm-Leach-Bliley Act; sales of hunting and fishing licenses; and sales of over-the-counter products containing pseudoephedrine.
- Serving in a leadership role in technology, be it online or offline. Some of these technologies have privacy implications, like online advertising, Radio Frequency Identification (RFID), or mobile devices.

Walmart

Simply put, Walmart has a deep engagement with the American public in a variety of contexts. Consequently, we respectfully submit to you that the Company has one of the deepest understandings of not only the dynamics of compliance with myriad privacy requirements, but also what we see as the underlying goals of what privacy is trying to accomplish for consumers. We have made it our business to understand what customers want.

Given the depth and breadth of Walmart's understanding of consumer privacy issues, we appreciate the Committee including Walmart in today's discussion, and would encourage you to engage other similarly situated companies in the discussion of these important issues. Since the emergence of online behavioral advertising as a topic of legislative and regulatory interest, we have been concerned that policymakers evaluating privacy issues may narrow their focus to the practices and concerns of leading Internet companies, with less involvement of other industries that face the same or equally challenging privacy issues. Indeed, efforts to understand and mitigate the potential privacy risks posed by behavioral advertising and the online use of personal information are framing much of the debate on privacy issues across the board. Some companies have begun to advocate for comprehensive privacy legislation. It is imperative that, as privacy rules are developed, legislators take the time to fully understand the impact to consumers and companies that have both online and offline relationships.

Walmart

That said, we certainly agree that behavioral advertising and the online tracking methods upon which it relies should be the subject of thoughtful scrutiny. To be sure, Walmart does have an interest in the issues that are of concern to online businesses – we are heavily engaged in that business ourselves. According to Hitwise, a service that measures online usage, Walmart.com is among the top five most visited ecommerce websites in 2009. As it relates to online advertising, we even use different models within the business. At samsclub.com, targeted online marketing is done within the four walls of the Sam's Club website. At walmart.com, in addition to such first-party ads, the company also participates in an advertising network to serve relevant advertising across the network, the practice often called online behavioral advertising.

At the same time, however, we submit that addressing the needs of one industry sector, or one channel such as online commerce, that excludes or is inconsistent with others, is short-sighted and may lead to skewed regulatory schemes. For the vast majority of U.S. businesses, this could be cumbersome at best and unworkable at worst, and may well not even address the underlying issues for consumers.

III. Principles-Based Approach

In considering how to regulate privacy effectively, Walmart favors a principles-based approach. We think this is the best way for privacy to work for companies and consumers. It also provides a good foundation to discuss global issues with other countries where business is international. Having a set of framework principles in place that can be applied in many

different contexts would provide an effective, consistent approach to privacy. A privacy regime based on a well-conceived set of principles could be applied to every new technology, every new marketing channel, and every new use of consumer information. Such a framework would impose coherent and predictable standards that are easily understood by both consumers and businesses. We cannot stress enough that the more coherent the standard, the more compliance will be achieved.

A principles-based approach to privacy is not new. Several years ago, the Fair Information Practice Principles were put in place to provide a framework for addressing privacy. These principles set forth a broad scheme regarding issues that even today remain at the forefront of the policy debate. The principles address the need for organizations to provide:

(1) Notice to consumers of an entity's information practices,

(2) Choice for consumers regarding how their information may be used,

(3) The ability of an individual to both access data about himself or herself and contest that data's accuracy and completeness,

(4) Information security, and

(5) Effective enforcement and redress.

While much has changed since the Fair Information Practice Principles were first articulated, they can provide a starting point from which to craft a modern framework. Focusing on core privacy principles in the U.S. would facilitate the creation of predictable

standards, and help avoid repeatedly dedicating time and energy to the creation of ad hoc laws to address emerging technologies.

While it may be possible to devise customized sets of laws to address privacy issues on an individualized, technology-specific basis, we question the efficiency – and, more importantly, the outcome – of such an approach. Not only does it create difficulties for companies attempting to develop an overarching approach to privacy, it also puts consumers in the position of having to navigate a confusing maze of unpredictable standards.

IV. Walmart Privacy Policy Efforts

As an example of a principle-based approach, this summer we updated our customer privacy policy for Walmart operations. The updated policy is based on the Fair Information Practice Principles, as well as developing industry standards and global guidelines. Our goal was to make the policy transparent, meet best practices, and to be integrated across all business units, online and offline, as well as all product offerings. We thought it would really help our customers to understand our privacy practices if we integrated them, rather than having separate policies for online and offline operations, and to have them all in one place. To further increase transparency, we included a short summary privacy notice that provides highlights of the privacy policy from which a customer can link through to the detailed privacy policy.

The new privacy policy provides customers more control over their data. Examples are:

Walmart

- Creating a preference center that allows customers to tell us directly their preferences regarding direct marketing and data sharing for marketing purposes.
- Moving to a stricter standard for data uses customers typically consider more sensitive. Walmart now uses an opt-in standard for telemarketing and data sharing with third parties for marketing purposes.
- Providing additional or enhanced opt-out mechanisms. Examples include ratings and surveys via email; prescreened offers of credit; and online behavioral advertising.
- Providing customers greater access to their own information, through their online accounts or otherwise.
- Providing more options to submit questions and concerns. We receive about 15 - 20 customer inquires a week about privacy, and are very timely in our response.

This initiative gave us further insights into how to focus on underlying privacy principles and then to operationalize them. With regard to online behavioral advertising, Walmart provides clear notices and opt-outs, consistent with the FTC Self-Regulatory Principles for Online Behavioral Advertising as well as developing industry best practices. Equally importantly in our view, we integrated our approach regarding online advertising into our larger view of privacy – when and how is it appropriate to give notice? When and how should consumer choice be offered?

Walmart

V. Consumer Notice and Choice

We would like to turn to these key aspects of privacy principles. We understand that a growing topic in the public policy debate is whether the traditional U.S. approach, including notice and choice, is still valid as technology, business practices, and consumer expectations evolve. We do believe that notice and choice still have a central place. This is not to say that there are no other protections to consider as a framework is developed. But we should not lose sight of some of the key ways that consumers interact with businesses. We offer the following examples to show the value of notice and choice, as well as how a broader principles-based approach is appropriate and needed, which can extend beyond the current debate about online activities and behavioral advertising. Walmart extensively develops and implements new technology. As one example, Walmart has begun programs or pilots with mobile messaging. These messages can alert customers that pharmacy prescriptions are ready for pick-up, or about special offers in store. Notice and choice are needed to make mobile interactions work.

Another illustrative example concerns our experiences with the use of Electronic Product Code (EPC) technology. At the simplest level, EPC is the next generation bar code. EPC is a unique identifier, which can signify any unique item, such as a case or pallet of products, or an individual product. EPC is typically placed on a tag, which can then be "read" by RFID. Currently, EPC benefits our company by tracking certain case and pallets in the supply chain, and benefits consumers through greater availability of merchandise.

When EPC may be offered on individual products on the sales floor, there will be more benefits to the company and consumers. Consumer benefits of online behavioral advertising are often discussed in terms of more focused and relevant advertising. These are certainly of value. But potential benefits of EPC to the customer are even more direct. To name just a few, EPC could facilitate the following: merchandise returns without receipts; automatic warranty activation; easier sortation of items for recycling; and product and food safety. Some day EPC could revolutionize check-out-lines.

While we know EPC will offer benefits, we understand that some customers may feel uncomfortable with the technology. Walmart has thus been building in privacy protections. As we develop EPC, Walmart follows the Guidelines on EPC for Consumer Products. The Guidelines were issued by GS1 EPCglobal, the standard-setting body for EPC, in 2003 with final adoption in 2005. We believe the Guidelines represent one of the first instances of applying privacy standards to technology and tackling some of these issues. As an example, the Guidelines are some of the earliest privacy guidelines to tackle how to extend privacy protections to non-personal information, as EPC tags used by retail contain no personal data.

As a cornerstone of EPC development, Walmart is designing its use to enable consumer choice. EPC tags will be easily removable from the product or its packaging, such as by placing the EPC tag on the price tag. If EPC tags used by the retail industry are ever embedded, we will offer a mechanism to disable the tag.

Walmart

We believe that choice is absolutely the right model for this technology. Some, perhaps most, consumers will appreciate the benefits provided by the technology. Some will not. But ultimately consumers should be able to choose which they prefer.

A challenge, of course, is how to provide appropriate notice. This covers both how consumers will know this technology is in operation – and also know what this technology actually means. A variety of methods and channels are possible, including notices on products themselves; notices on or in facilities; and website information. You can see how a debate that focuses solely on notice that can be provided on a website, like pop-up notices, would miss the boat for this technology.

IV. Conclusion

Walmart interacts with consumers frequently and in every conceivable way. A uniform, or at least consistent, privacy framework that includes standards such as consumer choice is effective both for consumers and businesses. Companies would be able to structure cohesive policies for protecting consumer privacy. A privacy regime based on a set of core principles would be sufficiently flexible to be applied in multiple contexts. Consumers deserve to know what to expect with regard to how their information is being collected and used, where they may obtain further details if they desire, and how they can make appropriate choices regarding the use of their data or technology. As additional protections are developed, a principle-based approach should help answer questions like how to make the

protections meaningful, and how far to extend them before they become attenuated and unworkable.

Thank you again for the opportunity to address **the Subcommittees.** Walmart looks forward to working with **the Subcommittees and the full Committee as you** move forward in shaping the privacy framework in the U.S.

APPENDIX

WALMART PRIVACY POLICY

Walmart

Privacy Policy Highlights

Scope:

This policy applies to Wal-Mart operations, both in stores and online, in the United States and Puerto Rico. Examples include Walmart Supercenters, Neighborhood Markets and Walmart.com.

Information We Collect:

Read more about Information We Collect.

We collect your information from the following sources:

- Information you give us, such as during transactions, customer service, surveys, and online registrations.
- Information from other sources, such as consumer reporting agencies, and
- Information automatically collected when you visit our websites, such as via cookies, and in stores, e.g. via video cameras.

How We Use and/or Share Your Information:

Read more about How We Use and/or Share Your Information.

- Walmart does not sell or rent your personal information to third parties.
- Walmart uses your information to provide products and services and to support core business functions. These uses include fulfillment, internal business processes, marketing, authentication and fraud prevention, and public safety and legal functions.
- We may combine all the information we collect. We may share your information with our corporate affiliates like Sam's Club (except for information you provide to purchase financial products).
- We may share your personal information with third parties under the following limited circumstances:
  - with service providers or suppliers that help with our business operations
  - with the financial institution who jointly offers a Walmart credit card
  - when necessary to protect the safety, property, or other rights of Walmart, its affiliates, customers, or associates, or when we believe in good faith that the law requires it.

Your Choices:

Read more about Your Choices.

We want to communicate with you in ways you want to hear from us. Examples include email newsletters, special offers, and new product announcements. We use the following standards for marketing communications:

- We will not contact you via phone or text message without your express consent (opt in),
- We will not share your information with third parties for marketing purposes, without your express consent (opt in),
- We use an opt-out standard for all other communications. This means we will conduct the activity unless you tell us not to.
- We participate in an ad network for some advertising on the site. This means that you may see advertising tailored to how you browse websites in the network. Learn more about the ad network, including how to opt-out.

You can provide us your marketing preferences by visiting the Privacy Preference Center or by contacting us below. The Preference Center allows you to update or change your preferences for marketing materials at any time.

How to Contact Us:

You may contact us as described in the Contact Us section below.

Important Information:

- We are committed to providing you a fair and timely response to any privacy concern or question you bring to us.
- We recognize the importance of privacy. It is more than an issue of compliance – it is one of trust. Read our entire privacy policy.
- Read more about the additional protections for sensitive information, such as health-related information or financial services.
- Visit Walmart's Privacy & Security Information Center for general tips and resources.

WALMART PRIVACY POLICY

Walmart recognizes the importance of information privacy. We believe that privacy is more than an issue of compliance – it is one of trust. We strive to manage your personal information in accordance with our basic belief of respect for the individual. This policy describes:

- How and why we collect your personal information.
- How your information is used and protected.
- When and with whom we share your information.
- The choices you can make about how we collect, use, and share your information.

We do not sell or rent your personal information to third parties. If you have any questions about our privacy policy, please contact us as described in the section entitled "Contact Us" below.

Notice and Scope of Our Privacy Practices

Walmart provides customers with clear, prominent, and easily accessible information about its privacy practices. This policy applies to Walmart operations, both in stores and online, in the United States and Puerto Rico. Examples include Walmart, Supercenters, Neighborhood Markets, and Walmart.com. Sam's Club has its own privacy policy for its members. Read more about the Sam's Club Privacy Policy.

Our Pledge of Accountability

Walmart expects our associates and business partners to manage your personal information properly and maintain your trust. We are accountable for complying with this policy and take reasonable and timely steps to ensure compliance.

Information We Collect

We collect personal information about you to deliver the products and services you request and to help improve your shopping experience. We do this using lawful and fair methods. We strive to limit the amount of personal information collected to support the intended purpose of the collection.

Information You Give Us
We collect personal information from you in a variety of ways when you interact with Walmart, both in stores and online. Some examples are when you:

- Create an account on one of our websites;
- Make an online or in-store purchase from us;
- Use a gift registry;
- Request check cashing, apply for credit, or purchase certain financial products;
- Conduct a transaction where we collect information required by law (such as the sale of pseudoephedrine);
- Request customer service or contact us;
- Submit a Walmart related story or testimonial;
- Participate in a contest, sweepstake, promotion, or survey; or
- Otherwise submit personal information to us.

Personal information is information that identifies you specifically. The personal information we collect may include contact and payment information like your name, email and physical addresses, phone numbers, and credit and debit card numbers. When you ask us to ship an order, we may collect information you provide us such as the name, address, and phone number of recipients. We may collect your Social Security Number where required for certain transactions, such as to purchase firearms, or to help provide credit or other financial products and services.

Information from Other Sources

We may receive personal information about you from other sources as well. Examples of these sources are entities that can help us correct our records, improve the quality or personalization of our service to you, and help prevent or detect fraud. In addition, we may collect information from consumer reporting agencies, affiliates, or other service providers if you apply for credit or purchase certain financial products.

Automated Information Collection
We receive and store certain types of information when you interact with our websites, emails, and online advertising. Our purpose is to allow the websites to work correctly, to evaluate use of the website, and to support website analytics and marketing campaigns. Some examples include:

- We may collect technical information such as your internet protocol address, your computer's operating system and browser type, the address of a referring website, if any, and the path you take through our web pages.
- We use "cookies" to recognize you as you use or return to our sites. This is done so that we can provide a continuous and more personalized shopping experience for you. A cookie is a small text file that a website or email may save to your browser and store on your hard drive.
- We may also use web beacons. Beacons allow us to know if a certain page was visited, an email was opened, or if ad banners on our website and other sites were effective.

We operate cameras in stores for security and operational purposes, such as to measure traffic patterns. When used for operational purposes, we do not use these cameras to identify you personally.

How We Use Your Information

Walmart uses your information to provide requested products and services and to support core business functions. These include fulfillment, internal business processes, marketing, authentication and fraud prevention, and public safety and legal functions. Some examples include:

- To fulfill your requests for products and services and communicate with you about those requests;
- To register and service your account;
- To administer surveys, sweepstakes, contests, and promotions;
- To provide customer service and alert you to product information, including recalls;
- To help us improve and customize our service offerings, websites, and advertising;
- To send you information about our products, services and promotions;
- To protect the security or integrity of our websites and our business; and
- With regard to credit qualification and applications.

To accomplish these purposes, we may combine personal and non-personal information we collect online with offline information, including information from third parties. We may also share your information within our family of corporate affiliates, including Sam's Club, to accomplish these and our affiliates' purposes. However, we do not share with affiliates information that you provide to purchase a financial product or service like check cashing, money orders, money transfers, or bill pay.

How We Share Your Information Outside Walmart

Walmart does not sell or rent your personal information to third parties. We may share your personal information, whether you are a current or former customer, only under the following limited circumstances.

Service Providers

We may share information about you with service providers or suppliers that help with our business operations. Examples are shipping vendors, billing and refund vendors, credit card processors, and companies that help us improve our product and service offerings and our websites. We require these service providers and suppliers to keep the information secure. We also prohibit them from using your information for any purposes other than those requested by us.

Credit Applications

If you apply for a Walmart credit card, such as a co-branded or private label card, we may share your information with the financial institution(s) that we partner with to offer the credit card. Our partner may only use the information you give to us to provide the credit card. Similarly, if you qualify for a credit account and are not offered credit by Walmart, we may share your information with our partner so that they may extend the offer of credit as required by law.

Legal Requirements and Protection of Our Company and Others

We may share your information in other special circumstances. These include situations when we believe in good faith that the law requires it or that the sharing is necessary to protect the safety, property, or other rights of Walmart, our customers, our associates, or any other person. Examples include protecting the health or safety of customers, or addressing crimes committed on Walmart property. Data from in-store security cameras may also be provided to law enforcement upon written request.

Marketing Purposes

Based only on your express consent, we may share information with carefully selected vendors who may offer you products and services of interest. You may opt-in to this sharing under the "Your Choices" section below.

Aggregate Information

We may share aggregate and statistical data that does not identify you personally. We may do this for research and marketing purposes, for instance to describe our services to prospective partners or advertisers, and for other lawful purposes.

Business Transfers

In the unlikely event that Walmart or substantially all of its assets are acquired by an unrelated third party, your personal information may be one of the transferred assets.

Your Choices

Marketing Preferences

We want to communicate with you in ways you want to hear from us. Examples are newsletters, special offers, and new product announcements. We use the following standards for marketing communications:

- We use an opt-in standard for phone and text messages. We also use an opt-in standard for sharing information with third parties for marketing purposes. Opt-in means we will only conduct the activity with your express consent.
- We use an opt-out standard for all other communications. Opt-out means we will conduct the activity unless you tell us not to.

You can provide us your marketing preferences by visiting the Privacy Preference Center. The Preference Center allows you to update or change your preferences about receiving marketing materials at any time.

Or you may contact us as described in the Contact Us section below.

If you contact us by email or mail, please be sure to include your full name, the types of communications you would like to receive or not receive, and your related contact information. For instance, if you would like to opt-out of mail, include your mailing address.

Please allow sufficient time for your preferences to be processed. It may take up to 10 days to process your requests related to email and 4-6 weeks for other requests. You can also change your mind about your marketing preferences. To do so, you can visit the Privacy Preference Center or contact us at one of the above addresses.

Please be aware that, even if you have opted out of receiving marketing communications from us, we may still contact you for transactional purposes. Some examples are contacts for customer service, product information, service or reminder notices, or recalls. We may also need to contact you with questions or information regarding your order, such as regarding order status, shipment, or refunds.

Credit offerings

The above marketing preferences do not apply to our credit card offerings since these are provided through our financial institution partner(s). However, you can choose to stop receiving prescreened offers of credit from all companies, including our prescreened offers, by calling 1-888-567-8688 or by going to www.optoutprescreen.com.

Online Operations and Advertising

You may exercise choices related to our online operations and advertising. For instance, you can choose to browse our websites without accepting cookies. Please know that cookies allow us to recognize you from page to page, and they support your transactions with us. Without cookies enabled, you will still be able to browse our websites, but will not be able to complete a purchase or take advantage of certain website features.

To learn more about cookies, including how to refuse cookies on your computer, follow these links:

- Microsoft Internet Explorer
- Netscape Navigator
- Mozilla Firefox
- Apple Safari
- All About Cookies

You may also opt-out of certain online advertising. Walmart.com participates in an ad network for some of the advertising found on the site. The ad network allows us to display advertisements that are tailored to your browsing interests on our websites and other sites. It also allows us to avoid sending you duplicate ads and to control the frequency of the ads you see. Walmart uses one or more partners to participate in the ad network. The partners use cookies, web beacons, or similar technologies to display these advertisements. We do not permit our ad serving partners to collect personal information about you on our websites. Rather, we provide them non-personal information about you such as browsing information like types of pages viewed and categories of interests. Our partners may use this information, as well as information they have collected when you are on other sites within their network, to help select which ads to display. We or our partners only retain ad network data for legitimate business purposes. Learn more about ad network business practices and the privacy policies of our partners. The information includes how to opt-out of participating in ad networks in this manner.

How to Access and Update Your Information

Walmart takes reasonable steps to keep your personal information accurate and complete, so we can treat your information properly and effectively under this policy. You can access or update your information, including contact or account information, in the following ways:

- If you have created an account on one of our websites, log into your account. Once you do, you will be able to enter and update your own contact information and payment information, as well as contact information for recipients you have designated.
- Contact us at the email or postal address listed in the "Contact Us" section of this policy. Please include your current contact information, the information you are interested in accessing, and your requested changes. We will provide you the information requested if reasonably available, or will describe the types of information we typically collect. We will make changes you request or will provide an explanation of what actions we will be able to take with regard to the request.
- If you need help accessing your information related to a financial product offered by a Walmart partner, we will assist you with that request if you contact us via the "Contact Us" section below.
- If you need assistance with your Optical or Pharmacy information, please visit the Pharmacy or Optical section below for instructions on accessing these records.

How We Secure Your Information

Securing your information is a company priority. Whether you are shopping online or in our stores, we use reasonable security measures to protect the confidentiality of personal information. When we do have to collect your most private personal information, such as Social Security Numbers, we will protect its confidentiality, prohibit its unlawful disclosure, and limit access to authorized personnel only.

Online Protections

Your account information is protected by the password you use to access your online account. Please keep this password confidential. We also use an encryption technology called Secure Sockets Layer (SSL). When you enter a secure portion of a website, you will see https (instead of http) in the address bar, and an image of a closed lock or a solid key should appear in the address bar or bottom bar of your browser window. If you click on this image, website security information will appear. This indicates that your personal information is transmitted in encrypted form, not to some unknown or unauthorized server. Walmart.com has also obtained a digital certificate from Verisign, Inc., a leading provider of Internet trust services.

Hard Copy and Electronic Storage Protections

Personal information that is maintained in our offices or stores is subject to physical, administrative, and technical controls as well. Hard copies of private information are maintained in locked locations or cabinets with similar restrictions for electronic storage of private information. When disposed of, the information is shredded, destroyed, erased, or otherwise made unreadable.

Privacy Protections for Specific Types of Information

Pharmacy and Optical Departments

When you use our Pharmacies or Vision Centers, you may provide us with your health information so that we may process your request. We understand the sensitive nature of such information and respect your privacy by keeping it confidential. This includes complying with federal law (the Health Insurance Portability & Accountability Act or HIPAA) and applicable state laws. Our Notice of Privacy Practices describes how we protect your information maintained by our Pharmacies and Vision Centers, and how you can access your records. A copy of the Notice of Privacy Practices is available online by visiting Pharmacy or Vision Center. A copy of the Notice is also provided to you by the Pharmacy or Vision Center at the first time of service, or can be requested at any time at your local Walmart.

Financial Products and Services

As you use Walmart financial products and services, the privacy of your personal information is protected under the federal Gramm-Leach-Bliley Act (GLB) and applicable state laws. Your personal information is protected whether you are a current or former customer. These financial products and services include money orders, money transfers, credit card offerings, bill payment, and check cashing.

Walmart provides you check cashing services directly. This privacy policy describes how we collect, use, disclose, and protect your information related to this service.

For all other services, we serve as an agent for suppliers to offer you financial products and services. Even though we are an agent for these services, we work with our partners to ensure they provide appropriate privacy policies and protections. Below is the list of our financial services partners, along with a link to their privacy policies:

- Credit Cards offered through GE Money Bank
- Money Transfers, Money Orders, and Express Bill Pay offered through MoneyGram
- Money Card offered through Green Dot and GE Money
- Bill Payment offered through CheckFreePay

We also protect the credit or debit card information we collect during transactions. We comply with industry requirements known as the Payment Card Industry Data Security Standards (PCI Standards). These standards require safeguards for handling and securing customer information. These include using secure networks; encryption or other protection of cardholder data; physical and technical access controls; monitors and tests of security systems; and information security policies.

Privacy of Children Online

We are committed to protecting children's online privacy. In order to protect children's personal information, and to meet the standards of the Children's Online Privacy Protection Act (COPPA), we do not knowingly collect personally identifiable information from children under the age of 13 on Walmart websites without prior parental consent.

Walmart.com is a general audience website not geared towards children. In several areas of Walmart.com, such as when customers contact us via email, create a Walmart.com account, or sign up for e-mail newsletters and alerts, we ask for birth year information. We ask for this to help us ensure that children do not provide us personal information on the site. Please contact us at the email or postal address provided in the "Contact Us" section of this policy if you believe we may have collected information from your child and we will work to delete it.

International

As a global company, Walmart has separate privacy policies for its international offices. When you give us personal information on a website or in a store, the information may be sent to servers outside of the country where you provided the information. Walmart takes steps to ensure that your information is treated securely and in accordance with this privacy policy or any privacy policy that applies to a Walmart international site or store where you provided your information.

Changes to the Walmart Privacy Policy

Please check our privacy policy periodically for changes. We will also notify you of significant updates and will post the date it was last updated at the bottom of the privacy policy.

Contact Us

Please feel free to contact us with any questions or comments about this policy or about how your information is handled. You can contact us via the addresses below:

Email:
Privacy@wal-mart.com

Mail:
Walmart Corporate
Privacy Office, MS #505
508 SW 8th Street
Bentonville, AR 72716-0505

Your California Privacy Rights

Our privacy policy describes how we share information for marketing purposes. The policy and rights apply to all customers, including California residents:

- We share information with others outside of Walmart only if we have your express consent (opt-in). See How We Share Your Information Outside Walmart.
- We also share information with other businesses within our corporate family, such as Sam's Club. See How We Use Your Information.

Please contact us with any questions, or to request a list of third parties to whom we may disclose information for marketing purposes and the categories of information we may disclose, via the Contact Us section above.

Effective: August 23, 2009

Mr. BOUCHER. Thank you very much, Ms. Strickland. Ms. Bougie.

STATEMENT OF MICHELLE BOUGIE

Ms. BOUGIE. Thank you, Mr. Chairman and members of the subcommittees. My name is Michelle Bougie, and I am the Senior Internet Marketing Manager of Learning Resources, Incorporated, of Vernon Hills, Illinois, a small business manufacturer and distributor of classroom materials and educational toys.

We sell both business to business and business to consumer, maintaining an extensive Web site and e-commerce store, as well as undertaking an active direct mail program for schools, teachers, and consumers.

In our business, the protection of consumer information is paramount. We have long maintained a detailed privacy policy, which is posted prominently on our Web site. Our commitment to the protection of consumer privacy is voluntary, but it is also required in the marketplace. Self-regulation by industry and market standards works effectively, and I urge you to be cautious in regulating the use of consumer data to avoid unintended consequences, that might put small businesses at a permanent market disadvantage, by preventing us from using technology to grow and expand.

In the last 12 years, I have worked with literally dozens of companies in various capacities relating to the use of consumer data. In my experience, industry voluntary privacy standards have been universally adopted and are a regular element of any commercial transaction, online or offline. Privacy is a routine and fundamental part of good business practices involving the sharing and use of consumer data today.

Industry voluntary privacy standards were developed to meet consumer expectations, and to match best practices from traditional direct mail. Companies who do not participate in self-regulatory practices, such as protecting consumers' financial information, or fail to follow opt-out instructions, are blacklisted by consumers.

As we all come to understand, the consumer is now more powerful online. Consumers use the power of social media to warn others about Web sites that offend or use bad practices. Consumers will, likewise, use the same tools to promote businesses that use best practices.

It is important to recognize the collection and use of consumer data is essential to improving the consumer experience online. Cookies and other tracking means were developed to make it possible to make targeted product and service offers that match consumer needs. This sophisticated information gathering process has created a $300 billion industry and 1.2 million jobs. We must be careful not to endanger this major source of jobs and enhanced consumer choice.

Consumers can control the collection of consumer data in many important ways. Many companies like ours offer the right to opt out for consumers, and choose to not participate in our marketing activities.

Opt-out options are far superior to opt-in options, both from the standpoint of businesses and consumers. Businesses prefer opt-

outs, because they believe that few consumers will ever opt-in, as fear alone discourages most people from opting in. Consumers have already experienced an online world filled with opt-ins. In the early days of the Internet, featured cautious approaches by Web sites with many opt-in choices. Consumers were prompted to accept Web site terms before entering, a practice that turned off many consumers at the early online experience, moved at a glacial pace, slowing the online purchase process for customers, and lowering revenues for businesses.

Consumers have ways to control the collection of data. Internet browser software can notify consumers of cookies, ActiveX controls, or other means of data collection. In order to maximize the speed and pleasure of their online experiences, many consumers turn off these warnings.

Again, consumers and businesses are making these privacy options and choices without the need for federal regulation. We believe that regulation of consumer data may sharply curtail our ability to grow, both online and offline. Small businesses don't generate enough leads to keep customer lists fresh and growing. We must have access to market data to find new customers.

Likewise, consumers need us to promote our products and services, because without this marketing, small businesses are just too hard to find.

If our ability to collect and use this data is curtailed, we are vulnerable to large businesses gaining an effective monopoly on consumer identities and preferences. Large businesses, with high web traffic, or many storefronts, have the means to generate and use consumer data for prospecting, to remain dominant. Small businesses will lose this game every time.

I urge you to be cautious and to carefully avoid unintended consequences. The Internet is a huge job creator, and one of the great drivers of today's complex and rapidly evolving economy.

A one size fits all solution is very dangerous in an economy of this complexity. We believe the new legislation should take a crawl, walk, run approach, focusing on the most sensitive data, such as financial information or healthcare data, and relying on opt-out mandates for routine commerce. By taking such a prudent approach, Congress can ensure that small businesses do not find themselves in a permanent federally mandated market disadvantage.

Thank you for considering my views on this subject. I am happy to answer any questions.

[The prepared statement of Ms. Bougie follows:]

House Committee on Energy and Commerce
Subcommittee on Communications, Technology, and the Internet
Subcommittee on Commerce, Trade and Consumer Protection
November 19, 2009

Re: Exploring the Offline and Online Collection and Use of Consumer Information

Statement of
Michelle Bougie
Learning Resources, Inc.
380 North Fairway Drive
Vernon Hills, Illinois 60061

STATEMENT OF MICHELLE BOUGIE
Senior Internet Marketing Manager
Learning Resources, Inc.
Vernon Hills, Illinois

Mr. Chairmen and Members of the Subcommittees, thank you for the opportunity to provide testimony on the implications of regulation of the collection and use of consumer information for the small business community. My name is Michelle Bougie and I am the Senior Internet Marketing Manager of Learning Resources, Inc. of Vernon Hills, Illinois, a manufacturer and distributor of educational materials and educational toys. We employ 150 people and sell our products in over 80 countries. We maintain a website with a web store and also have a direct mail program for schools and teachers and for consumers.

At our company, we take the privacy of our customers very seriously. We have long had a clear privacy policy available for consumers to review online, and provide various opt-out options for consumers who choose to not participate in our marketing activities. In addition, we offer consumers the ability to review and comment on the information we gather. This is standard industry practice and is intended to build confidence in the products and services we offer. Our Privacy Policy is available online at http://www.learningresources.com/category/customer+service/privacy+and+security.do.

We developed our privacy policy based on our review of Federal and State law, as well as voluntary industry practices such as the recommendations of the Direct Marketing Association. We also must make sure our policies are competitive with other merchants. These privacy practices are a necessary part of being a trusted supplier to our customers, as well as to remain competitive in the evolving e-commerce marketplace.

Our company has used consumer information in many ways over the years. In direct mail, it is customary to "rent" or exchange names and addresses for prospecting based on various

criteria that the owner of the lists has accumulated, such as date of last purchase, kinds of products purchased, home location, job title, and so on. The lists of names remain the property of the list provider (it is their valuable intellectual property), so in direct mail, we cannot retain the names – and normally don't even see them.

In the online world, we use data that we develop, or gain access to data maintained by other companies, to make targeted offers to prospective customers. The online "ad word" market depends on having access to consumer behaviors. Various providers present opportunities to make targeted offers or pay-to-click advertisements based on consumer data. Again, these data are useful for broadening the market for our products and services.

As a small business, we are concerned about possible regulation of online and offline collection and use of consumer information. There are several reasons for this concern:

a. **Small Businesses Need Access to Consumer Data to Grow.** The use of consumer data for marketing purposes is as old as mail itself. Direct mail companies rent or exchange names and addresses to facilitate company growth. This value-added, cost-effective process allows direct mail to be competitive with physical stores and to keep costs low while contributing to a higher standard of living for all Americans.

Prospecting with consumer data is not a one-sided opportunity for the business community. Our ability to reach customers interested in our products and services adds value to consumer choices and keeps the cost of product acquisition as low as possible. The greatest challenge a small business faces is finding those people who can benefit from its products and services. By the same token, many consumers have a hard time finding niche manufacturers focused on their needs. Through the use of consumer data, small businesses are able to reach across the entire economy to match up with consumers who want their products and services but may have never known where to get them. For an education company like ours, the urgency is real – many of our customers are school teachers or parents of special needs children. The

markets we sell into are small niches with very specific, technical needs. Consumers in these niches very often feel isolated and in some cases, abandoned. It is important that they have the option to consider our wares – it could make all the difference to a special needs child.

b. **Mass Market Competition Would be Overwhelming without Access to Consumer Data.** Many small businesses start in a bedroom, a garage, the trunk of a car. How does a great idea go from the dining room table to an organization of hundreds or even thousands of people? Small businesses go through a delicate winnowing process as they fight their way upstream against much larger, better-capitalized competitors. One of the serious natural disadvantages of small businesses is access to consumer data, which we are dependent on to grow our business, as we are too small to generate this information efficiently ourselves. Mass market companies who are able to use their large market footprint or high store count to operate independently of other people's data enjoy an inherent advantage over small businesses who need this data to "prospect". It is the exceptional small business that has the means to generate sufficient prospecting data to grow consistently.

To compensate for this deficiency, a marketplace developed to make this data available for use. Small business must acquire the right to use consumer data, such as names and addresses or buying patterns, to compete with much larger entities that generate or control that data themselves.

We have considerable fear that legislation to protect consumer privacy will create insurmountable advantages for larger companies who accumulate and use consumer data in their own businesses. It is not enough to distinguish between First Party and Third Party uses of consumer data. In today's economy, there are many vertically-integrated companies designed to exploit the value of consumer data entirely within their own selling organizations. If we cannot rent, access or use similar market data, those larger companies will be granted a form of monopoly that could devastate small businesses and give them unprecedented control over

consumers. Privacy legislation, if designed the wrong way, could make this disadvantage permanent.

c. **Consumers Have Not Objected To Our Privacy Practices.** We have long offered consumers the right to opt out of our data collection and use practices. This option is seldom used and, likewise, we seldom receive consumer complaints. Our consumers have not told us to change our policies, even though the Internet has put the consumer in charge.

Notably, the security of certain information, like financial information, medical information, sexual preference, etc., must be preserved, but is frankly not an issue in our businesses. Again, consumers have not expressed concern over our handling of this sensitive data.

The possible regulation of consumer information collection and use may create a new form of tort, exposing small businesses to new liability and litigation expense. Managing a new kind of tort liability is a distraction that small business owners do not need, and may not be able to afford. In our experience, the voluntary practices of the industry have proven powerful and effective. The introduction of new liability may only create a disincentive to trade and act as a significant market depressant that would further hurt small business.

d. **Opt-in's Have Limited Value.** We currently offer an opt-out option for consumers who don't want to participate in our marketing programs or data collection efforts. This method is endorsed by the Direct Marketing Association and has proven satisfactory to our customers. Opt-in methods may be suitable for certain sensitive data that could be used to commit fraud or identity theft, such as credit card information, or protected data like health care information, but would considerably reduce the accumulation of usable marketing data if applied to all consumer data. Nevertheless, it is essential that small businesses have access to other companies' data to prospect and expand their customer ranks. If accumulation of data in the market is reduced because of privacy legislation or if our access to third party data is truncated,

the ability of small businesses to compete and grow, by reaching consumers who really need our products and services will be substantially reduced. Consumers, in turn, will also find it harder and more expensive to find the products or services they need.

We believe most consumers facing a possible "opt-in" choice do not understand the mechanics of a direct marketing business, and thus would be suspicious of any request to accumulate or use consumer data. Even though it is innocuous, it may sound ominous. We believe most consumers would decline an opt-in choice because they would not understand the value they receive by participating in these programs. For this reason, we believe an opt-out option is by far the better choice.

It is worth noting that the National Do Not Call Registry is an opt-out program. See https://www.donotcall.gov/. The program gives consumers the power to stop unsolicited telemarketing calls, but they must first take simple, positive action to be excluded. Clearly, if Americans had to opt-in for telemarketing calls, the entire telemarketing industry would be jeopardized. No one would volunteer for telemarketing calls. The same issue confronts small businesses in the regulation of the collection and use of online and offline consumer data.

Recommendations and Conclusion:

We recommend that industry self-regulation be encouraged and relied upon. The current practices on the Internet and by direct marketing merchants provide strong protection to consumers. In addition, these guidelines are sensitive to individual needs and have evolved as the marketplace has changed, with marketplace forces keeping these practices sharp and competitive. Unless these mechanisms fail consumers, it is far more efficient and less economically burdensome to allow the effective industry self-regulation process to continue.

If Congress elects to regulate the collection and use of consumer data for marketing purposes, it must be careful to avoid unintended consequences. The economy is both highly complex and rapidly changing. The risk of broad scale changes in the privacy rules is creation of

a federally-mandated disadvantage for the small business community in the online and direct mail marketplace. This would hurt job creation and the vibrancy of the economy. We urge Congress to take a "crawl, walk, run" approach by taking limited action now. The example of the Do Not Call Registry, an opt-out mechanism, is a good way to start, if further regulation is deemed necessary.

Thank you for considering my views on this important subject.

Mr. BOUCHER. Thank you very much, Ms. Bougie.
Ms. BOUGIE. Thank you.
Mr. BOUCHER. Ms. Dixon.

STATEMENT OF PAM DIXON

Ms. DIXON. Thank you. I would like to thank the chairmen for inviting me here today. I am Pam Dixon. I am Executive Director of the World Privacy Forum.

We are a nonprofit, public interest research group, based in California. We focus on in-depth research of privacy issues.

The online and offline collection of information from consumers matters, because it impacts our lives, whether we know it or not. In the past, consumers have been told, you better watch out, because you have got to act a certain way, because something might go in your permanent record. We heard this in school, when we were young. But today, because of the large commercial databases, and those activities related to those commercial databases, we have a new kind of permanent record. I call this the modern permanent record.

This is a permanent record compiled from rich online and offline resources, and it can be used to deny or offer benefits, services, and goods and information to consumers.

What I would like to do is talk about how these commercial databases can be used to create a very detailed picture of a consumer, and what that picture can do to a consumer's life. And to do that, I would like to walk you through how the modern permanent record is created and used.

So, first, one source for the modern permanent record is marketing lists and databases. These are typically sourced from highly identifiable data. We are not talking about pseudonymous data residing on a hard drive somewhere. We are really talking about data where someone knows your name.

If you can look at the monitor, you will see a list of 20 million consumers. This is an ailments list, and it is a data card that is being sold on consumers. It lists detailed demographic information, and it also lists the various diseases that they have. This list is an unregulated list. It is outside of HIPAA, because these people gave their information up in some way or another, sometimes with more knowledge than another.

In the next list, you will see it is a list of mental health sufferers. This is a list of 3 million consumers who landed on a telemarketing list, or a list like this, and it talks about 2 million with anger, antisocial diseases, ADD, ADHD, autism, bipolar, and so forth. And the company says these people, marketing to them is, they are extremely receptive to any campaign, because they suffer from various mental problems.

And the real impact of these kinds of lists, that are so unregulated, is being seen already today. It is not theoretical. So, for example, one 91-year-old elderly vet was profiled in the New York Times. He landed on one such list, and what happened is his, he filled out a sweepstakes form, and he landed on a telemarketing list. It was sold, and as a result of bad actors purchasing the list, he was bilked of his life savings. And this gentleman, once he was

on the list, he had no effective rights to remove himself from the list, or mitigate those issues.

Another way that the modern permanent record is created is through what I call non-Fair Credit Reporting Act databases, or noncredit databases. These are databases that have rich scores of information in them. However, they may, even if they have identical information to what could be contained in a database subject to the FCRA, they are not subject to the FCRA, because they are used for different purposes.

An example of this is the Badcustomers database, and we have a screenshot of that Web site. That Web site says: "Are your purchasing transactions being denied? Find out if you have been blacklisted before it is too late." This database has 6 million consumers on it right now, and it has only been in existence for about a month. And the way consumers land on this database is that they dispute charges to their credit account.

Now, if that sounds familiar, it is because identity theft victims must dispute charges on their credit cards to move forward with their lives. So, these are the kinds of databases where yes, you disputed a charge, but what does that actually mean? Was it because you were a victim of fraud, or because you were a bad actor? This is a very difficult thing.

The third way that the modern permanent record is compiled and created is through a newer type of database, behavioral and transactional databases. These are the databases that put the 3–D into the consumer. They provide the real detailed picture of the consumer, and put flesh on the bones of the consumers.

An example of this is eye gaze tracking cameras in retail stores. These cameras are not visible to consumers. What they do is they track, basically, the number of consumers that have walked by certain points in the store. They also identify what the consumer is looking at, and for how long. But what has happened, at least in the past year, is that this type of technology has been also combined with facial recognition technology. So, what happens is that the consumer walking down the store, who is being captured by the eye gaze tracking camera is also recognized and then marketed to.

Now, that is a practice that is in use today. Everything that I have told you is in use today, and it is not theoretical. So, the question this committee has to face is, is it worth the risk involved to consumers, when you have these large, aggregated pictures of consumers that can define their lives. Is it worth that risk to leave them unregulated?

And I would argue that the modern permanent record, unless there are substantive rules of the road that govern how the modern permanent record is used, that will really creating a situation where there is going to be car accidents and pileups.

As consumers become more aware of the threat of how a modern permanent record can potentially be used in their lives, I think we really enter a situation where it can chill commerce, and really chill people's lives and inhibit them.

A good example of this can be found through Cox Communications. They offer a digital telephone service. That digital telephone service is then subject to detailed analysis, and what it does is it analyzes the numbers of, the phone numbers that you call and who

calls you. Well, there is nothing wrong with that, but what if you have a family member who is a deadbeat? What if you have a friend who is a deadbeat? What inference is drawn on you based on those phone calls?

So, what does that do to your permanent record, your modern permanent record, and that is really the question that we need to look at, and we need to answer, in terms of policy creation.

Thank you for your time, and I look forward to any of your questions.

[The prepared statement of Ms. Dixon follows:]

Testimony of Pam Dixon
Executive Director, World Privacy Forum

Before the Subcommittee on Communications, Technology, and the Internet, and the Subcommittee on Commerce, Trade, and Consumer Protection of the House Committee on Energy and Commerce

The Modern Permanent Record and Consumer Impacts from the Offline and Online Collection of Consumer Information

November 19, 2009

Chairman Boucher, Chairman Rush, and Members of the Committees, thank you for the opportunity to testify today about the online and offline collection of consumer information and what that means to consumers' everyday lives. My name is Pam Dixon, and I am the Executive Director of the World Privacy Forum. The World Privacy Forum is a 501(c)(3) non-partisan public interest research group based in California. Our funding is from foundation grants and individual donations. We focus on conducting in-depth research on emerging and contemporary privacy issues as well as on consumer education.

I have been conducting privacy-related research for more than ten years, first as a Research Fellow at the Denver University School of Law's Privacy Foundation where I researched privacy in the workplace and employment environment, as well as technology-related privacy issues such as online privacy. While a Fellow, I wrote the first longitudinal research study benchmarking data flows in employment online and offline, and how those flows impacted consumers.

After founding the World Privacy Forum, I wrote numerous privacy studies and commented on numerous regulatory proposals impacting privacy as well as creating useful, practical education materials for consumers on a variety of privacy topics. In 2005 I discovered previously undocumented consumer harms related to identity theft in the medical sector. I coined a termed for this activity: medical identity theft. In 2006 I published a groundbreaking report introducing and documenting the topic of medical identity theft, and the report remains the definitive work in the area. I will publish a new report on this issue in January 2010, as well research and consumer education pieces about other online and offline privacy issues.[1]

Beyond my research work, I have published widely, including seven books on technology issues with Random House, Peterson's and other large publishers, as well as more than one hundred articles in newspapers, journals, and magazines.

---

[1] Much of my privacy-related research work and writings are available at the World Privacy Forum web site, <http://www.worldprivacyforum.org>.

I am particularly interested in developments related to online and offline data flows of consumer information. Given the advances in technology that have significantly broadened and deepened the scope of consumer data collection practices, and given the new ways that these technologies and practices can shape and impact an individual's experiences and opportunities, I believe the decisions that this Committee arrives at will be of lasting importance. Given the transition our society is undergoing from analog to digital, it is crucial to question what changes the new environment brings, what new controls it includes, and its meaning for our day-to-day lives. It is especially crucial to carefully examine and to discuss the effects these developments will have for the consumer. We must look for a fair balance between benefit, risk, and harm.

The merging of offline and online data is creating highly personalized, granular profiles of consumers that affect consumers' opportunities in the marketplace and in their lives. Consumers are largely unaware of these profiles and their consequences, and they have insufficient legal rights to change things even if they did know.

Uncontrolled collection and accretion of information about our lives gathered from multiple sources online and offline over a course of time brings forward many complex issues, particularly those relating to privacy. I will turn to discuss these issues now.

I. The Modern Permanent Record: What Consumers Don't Know Can in Fact Hurt Them

Consumers don't have the ability to see or understand the information that is being collected about them,[2] and they don't have the tools to see how that information is impacting the opportunities that are being offered – or denied – to them. This is largely due to the little-known commercial structures and methods that have evolved to collect consumer data. These activities are extremely sophisticated and complex. They often defy consumer expectations of privacy, particularly when used to compile records and facts that become a defacto "**modern permanent record**" that follows consumers around and influences the quality of their lives, often without their knowledge.

A. The Evolution of New Consumer Information Collection Structures and Why It Matters

In the past, detailed consumer information was largely the provenance of credit bureaus. Now the emphasis has shifted from the credit reporting system to other areas, in particular **unregulated consumer reporting and data collection both online and off**. These newly evolved data collection and use models merge online data collections and offline data collections to form an informational picture of the modern consumer that is profoundly detailed, comprehensive, and may be used to determine a great deal about a consumer's experience and opportunities.

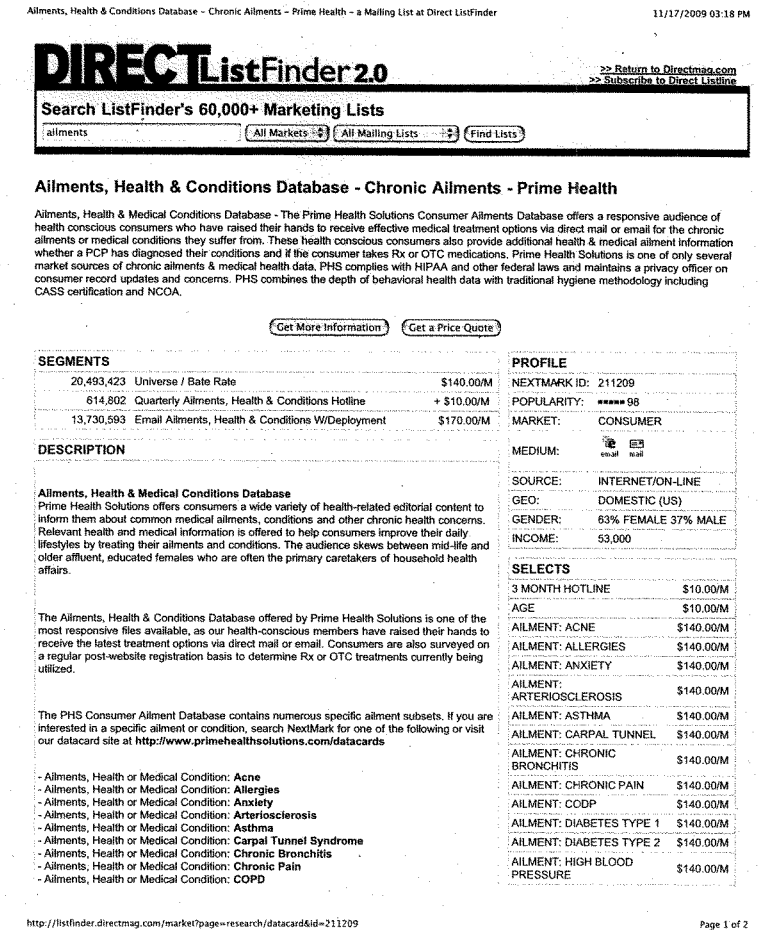
---

[2] See, for example, a new Carnegie-Mellon study on one aspect of consumer data collection, behaviorally targeted online ads. This study found that "many participants have a poor understanding of how Internet advertising works, do not understand the use of first-party cookies, let alone third-party cookies, did not realize that behavioral advertising already takes place, believe that their actions online are completely anonymous unless they are logged into a website, and believe that there are legal protections that prohibit companies from sharing information they collect online." Aleecia M. McDonald and Lorrie Faith Cranor, Carneigie Mellon University, *An Empirical Study of How People Perceive Online Behavioral Advertising*, Nov. 10, 2009.

The consumer data and the merged data infrastructure may offer benefits, but the same information may also be instrumental in creating consumer harms.[3] Note a current marketing list of 20 million consumers and their medical ailments (Figure 1). These consumers landed on this **Ailments, Health & Conditions list** because they supposedly wanted to receive via email or direct mail "effective treatment options" for the conditions they suffer from. These are identifiable consumers who can be targeted by their asthma or their heart disease, and also by

[3] See for example Karen Blumenthal, *How Banks, Marketers Aid Scams*, Wall Street Journal, July 1, 2009, available at <http://online.wsj.com/article/SB10001424052970204556804574260062522686326.html>.

their gender, education, and other characteristics.



Ailments, Health & Conditions Database - Chronic Ailments - Prime Health - a Mailing List at Direct ListFinder 11/17/2009 03:18 PM

DIRECT ListFinder 2.0

>> Return to Directmag.com
>> Subscribe to Direct Listline

Search ListFinder's 60,000+ Marketing Lists

ailments | All Markets | All Mailing Lists | Find Lists

Ailments, Health & Conditions Database - Chronic Ailments - Prime Health

Ailments, Health & Medical Conditions Database - The Prime Health Solutions Consumer Ailments Database offers a responsive audience of health conscious consumers who have raised their hands to receive effective medical treatment options via direct mail or email for the chronic ailments or medical conditions they suffer from. These health conscious consumers also provide additional health & medical ailment information whether a PCP has diagnosed their conditions and if the consumer takes Rx or OTC medications. Prime Health Solutions is one of only several market sources of chronic ailments & medical health data. PHS complies with HIPAA and other federal laws and maintains a privacy officer on consumer record updates and concerns. PHS combines the depth of behavioral health data with traditional hygiene methodology including CASS certification and NCOA.

Get More Information | Get a Price Quote

SEGMENTS

20,493,423	Universe / Bate Rate	$140.00/M
614,802	Quarterly Ailments, Health & Conditions Hotline	+ $10.00/M
13,730,593	Email Ailments, Health & Conditions W/Deployment	$170.00/M

DESCRIPTION

Ailments, Health & Medical Conditions Database
Prime Health Solutions offers consumers a wide variety of health-related editorial content to inform them about common medical ailments, conditions and other chronic health concerns. Relevant health and medical information is offered to help consumers improve their daily lifestyles by treating their ailments and conditions. The audience skews between mid-life and older affluent, educated females who are often the primary caretakers of household health affairs.

The Ailments, Health & Conditions Database offered by Prime Health Solutions is one of the most responsive files available, as our health-conscious members have raised their hands to receive the latest treatment options via direct mail or email. Consumers are also surveyed on a regular post-website registration basis to determine Rx or OTC treatments currently being utilized.

The PHS Consumer Ailment Database contains numerous specific ailment subsets. If you are interested in a specific ailment or condition, search NextMark for one of the following or visit our datacard site at **http://www.primehealthsolutions.com/datacards**

- Ailments, Health or Medical Condition: **Acne**
- Ailments, Health or Medical Condition: **Allergies**
- Ailments, Health or Medical Condition: **Anxiety**
- Ailments, Health or Medical Condition: **Arteriosclerosis**
- Ailments, Health or Medical Condition: **Asthma**
- Ailments, Health or Medical Condition: **Carpal Tunnel Syndrome**
- Ailments, Health or Medical Condition: **Chronic Bronchitis**
- Ailments, Health or Medical Condition: **Chronic Pain**
- Ailments, Health or Medical Condition: **COPD**

PROFILE

NEXTMARK ID:	211209
POPULARITY:	▪▪▪▪▪ 98
MARKET:	CONSUMER
MEDIUM:	e-mail, mail
SOURCE:	INTERNET/ON-LINE
GEO:	DOMESTIC (US)
GENDER:	63% FEMALE 37% MALE
INCOME:	53,000

SELECTS

3 MONTH HOTLINE	$10.00/M
AGE	$10.00/M
AILMENT: ACNE	$140.00/M
AILMENT: ALLERGIES	$140.00/M
AILMENT: ANXIETY	$140.00/M
AILMENT: ARTERIOSCLEROSIS	$140.00/M
AILMENT: ASTHMA	$140.00/M
AILMENT: CARPAL TUNNEL	$140.00/M
AILMENT: CHRONIC BRONCHITIS	$140.00/M
AILMENT: CHRONIC PAIN	$140.00/M
AILMENT: CODP	$140.00/M
AILMENT: DIABETES TYPE 1	$140.00/M
AILMENT: DIABETES TYPE 2	$140.00/M
AILMENT: HIGH BLOOD PRESSURE	$140.00/M

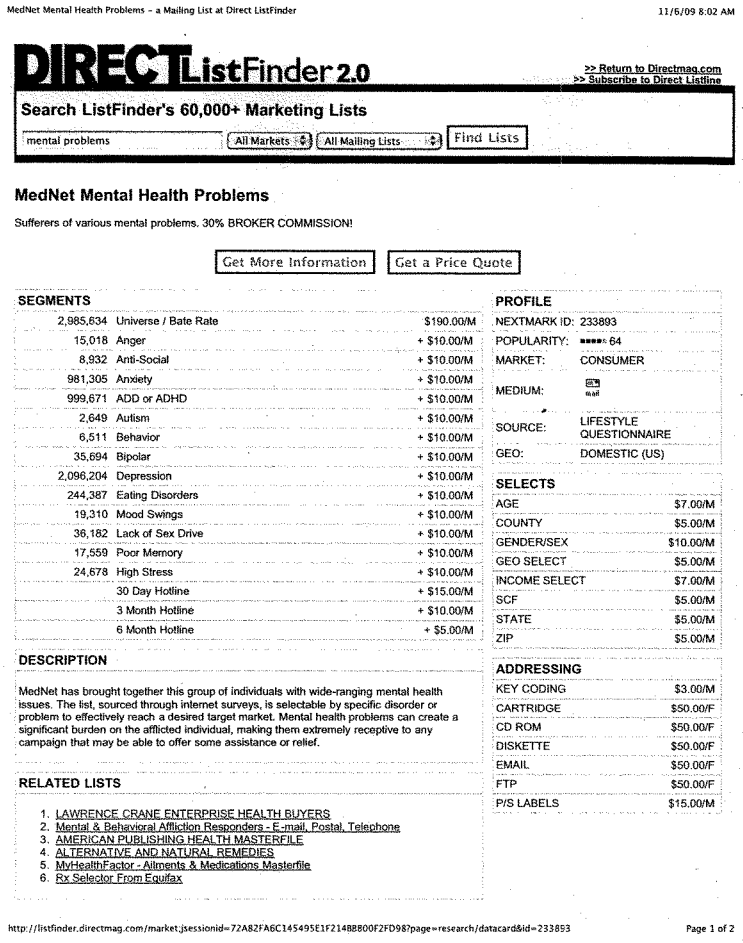
http://listfinder.directmag.com/market?page=research/datacard&id=211209 Page 1 of 2

Figure 1

Another example of this kind of consumer data collection activity, a current marketing list of consumers who are believed to have mental illness, can be seen in Figure 2. In this list, the **MedNet Mental Health Problems List**, you will see that individual consumers have been

segmented or identified by age, income, gender, and more. These are not pseudonymous numbers on a computer somewhere that must be linked with other information in order to identify a consumer.

This is already identifiable consumer data that is potentially harmful to those nearly 3 million consumers listed as having anxiety, eating disorders, poor memory, autism or other conditions. This list is sourced through Internet surveys, an online modality, but the list can potentially impact consumers' offline lives.



MedNet Mental Health Problems - a Mailing List at Direct ListFinder 11/6/09 8:02 AM

DIRECT ListFinder 2.0

>> Return to Directmag.com
>> Subscribe to Direct Listline

Search ListFinder's 60,000+ Marketing Lists

mental problems | All Markets | All Mailing Lists | Find Lists

MedNet Mental Health Problems

Sufferers of various mental problems. 30% BROKER COMMISSION!

Get More Information | Get a Price Quote

SEGMENTS

2,985,634	Universe / Bate Rate	$190.00/M
15,018	Anger	+ $10.00/M
8,932	Anti-Social	+ $10.00/M
981,305	Anxiety	+ $10.00/M
999,671	ADD or ADHD	+ $10.00/M
2,649	Autism	+ $10.00/M
6,511	Behavior	+ $10.00/M
35,694	Bipolar	+ $10.00/M
2,096,204	Depression	+ $10.00/M
244,387	Eating Disorders	+ $10.00/M
19,310	Mood Swings	+ $10.00/M
36,182	Lack of Sex Drive	+ $10.00/M
17,559	Poor Memory	+ $10.00/M
24,678	High Stress	+ $10.00/M
	30 Day Hotline	+ $15.00/M
	3 Month Hotline	+ $10.00/M
	6 Month Hotline	+ $5.00/M

PROFILE

NEXTMARK ID:	233893
POPULARITY:	■■■■■ 64
MARKET:	CONSUMER
MEDIUM:	mail
SOURCE:	LIFESTYLE QUESTIONNAIRE
GEO:	DOMESTIC (US)

SELECTS

AGE	$7.00/M
COUNTY	$5.00/M
GENDER/SEX	$10.00/M
GEO SELECT	$5.00/M
INCOME SELECT	$7.00/M
SCF	$5.00/M
STATE	$5.00/M
ZIP	$5.00/M

DESCRIPTION

MedNet has brought together this group of individuals with wide-ranging mental health issues. The list, sourced through internet surveys, is selectable by specific disorder or problem to effectively reach a desired target market. Mental health problems can create a significant burden on the afflicted individual, making them extremely receptive to any campaign that may be able to offer some assistance or relief.

ADDRESSING

KEY CODING	$3.00/M
CARTRIDGE	$50.00/F
CD ROM	$50.00/F
DISKETTE	$50.00/F
EMAIL	$50.00/F
FTP	$50.00/F
P/S LABELS	$15.00/M

RELATED LISTS

1. LAWRENCE CRANE ENTERPRISE HEALTH BUYERS
2. Mental & Behavioral Affliction Responders - E-mail, Postal, Telephone
3. AMERICAN PUBLISHING HEALTH MASTERFILE
4. ALTERNATIVE AND NATURAL REMEDIES
5. MyHealthFactor - Ailments & Medications Masterfile
6. Rx Selector From Equifax

http://listfinder.directmag.com/market;jsessionid=72A8ZFA6C145495E1F214BB800F2FD98?page=research/datacard&id=233893 Page 1 of 2

Figure 2

How did we arrive at a place where consumers can find themselves identified, and their information bought, sold, traded, and compiled on such lists … without their knowledge? These lists are the most visible portions of the large market that exists for consumer data, a market that is typically and intentionally obscured from our view. I would, for example, challenge any list

broker or commercial data broker to allow consumers to become aware of which of these lists they are on, to what companies their names have been sold, or how many times a list has been used for marketing data to them based on the information contained in the list. I would also challenge any commercial data broker to *fully* reveal consumers' complete modern permanent record for view in its totality.

The lists in Figures 1 and 2 are two small examples of a visible piece of the consumer data collection infrastructure. To understand the broader problem it is important to look at all of the consumer data collection pieces and how they fit together. To do that, I would like to walk you briefly through other pieces of this modern puzzle and how they work together to create highly individualized records of consumers.

B. Non-credit (Non FCRA) consumer databases

Non-credit, unregulated consumer reporting is a well-established business model, and has been for many years now.[4] Most consumers only find out about these databases accidentally, if at all. These are databases that contain robust and sensitive consumer information, for example, financial information or employment information. But this information is not used for purposes that fall under the Fair Credit Reporting Act, so the databases are completely unregulated. None of this is new.

What is new and has changed within the past decade is the ease of implementing this consumer data collection model. Collecting, accessing, and manipulating these types of data stores has gotten cheaper and faster. In the past, consumer information that was based on non-credit, unregulated reporting was controlled to some degree by expense of obtaining the data and the challenge of managing the databases. But now, technological advances have lowered many of the barriers.

Now there are more non-credit consumer databases in use, the databases are being used in new ways, and they are generally more accessible to more of the population. One can see this phenomenon on web sites such as Zabasearch.com.[5] There and at other similar web sites, anyone can purchase a robust file with detailed personal information about almost any individual over the Internet at minimal cost. The barriers to purchasing this information can be quite low. Often based on public record information, these files or dossiers provide basic identity, location, and

---

[4] Non-FCRA consumer databases may contain nearly identical information as a database that would be regulated under the FCRA, however, they are not used for FCRA purposes, therefore do not fall under the statute. These databases take on a wide variety of characteristics, ranging from anti-fraud to marketing to identity verification. Some examples include: Fair Isaacs FICO Falcon Fraud Manager < http://www.fico.com/en/Products/DMApps/Pages/FICO-Falcon-Fraud-Manager.aspx> This database analyzes detailed financial information of more than 1.8 billion accounts for fraudulent activity. Other kinds of non-credit databases contain large amounts of detailed information about consumers. See Acxiom's Consumer Insight Products databases, <http://www.acxiom.com/products_and_services/Consumer%20Insight%20Products/Pages/Consumer%20Insight%20Products.aspx> which offers "Deep consumer insights — in the form of Acxiom's data enhancements, lists, demographics, segmentation and buying behavior...". The Work Number, < http://www.theworknumber.com/> is a consumer database designed to verify income and employment, among other things.

[5] <www.zabasearch.com>.

history information about individuals. Again, this is not anonymous information whatsoever. It is a permanent record, with varying degrees of granularity or personalization.

These databases are one large piece of the consumer data collection picture.

C. Consumer behavior and transactional data collection, online and off

Another important piece of the consumer data collection machine is the bevy of databases containing detailed consumer **behavior patterns** and **consumer transactions**. These rich databases fill in the gaps of plain demographic information with a more three-dimensional picture of an individual. Activities that seemed so banal in the analog world – grocery shopping in a brick and mortar store, browsing books at a bookstore, looking up information about a medical condition in a paper Merck Manual and chatting about it with a close friend – these activities are now occurring increasingly digitally.

This makes it easy for these activities to be captured, stored, classified, and cataloged into behavioral profiles, which then become part and parcel of a *modern permanent record.* If you buy a certain book and if you visit certain web sites all of the time and if you travel frequently and if you visit certain stores – all of that goes into the modern-day version of the "permanent record" school teachers used to warn students about.[6]

This highly analyzed and massaged data that has been taken from multiple sources and possibly even collected over long periods of time can be used in various ways in consumers' lives. It is important to stress that due to the complex data merging between completely identifiable consumer information on marketing lists and previously non-identifiable information from, for example, online sources, that companies can have or find many ways of acquiring quite detailed information about people.

For example:

- An elderly veteran was bilked of his savings after he entered a sweepstakes and his name appeared on a marketing list. The list was sold by commercial data broker InfoUSA to a group of thieves, who then used the information to greatly harm him and other individuals. The story, which appeared in the New York Times, details the data trail of the veteran's information as it was sold to criminals and then used to defraud him.[7]

> "InfoUSA advertised lists of "Elderly Opportunity Seekers," 3.3 million older people "looking for ways to make money," and "Suffering Seniors," 4.7 million people with cancer or Alzheimer's disease. "Oldies but Goodies" contained 500,000 gamblers over 55 years old, for 8.5 cents apiece. One list said: "These people are gullible. They want to believe that their luck can change."

---

[6] Daniel Solove's book, The Digital Person, offers an important and extended discussion of how people now leave "digital breadcrumbs" as they live normal contemporary lives. The book offers an excellent legal analysis of the implications of what this means now and in the future. Solove, Daniel J. The Digital Person: Technology and Privacy in the Information Age. NYU Press, 2004.

[7] Charles Duhigg, *Bilking the Elderly with a Corporate Assist*, New York Times, May 20, 2007. <http://www.nytimes.com/2007/05/20/business/20tele.html?_r=1>.

> As Mr. Guthrie sat home alone — surrounded by his Purple Heart medal, photos of eight children and mementos of a wife who was buried nine years earlier — the telephone rang day and night."

What began as a sweepstakes response ended with a real individual on a list, which allowed him to be categorized and then sold to the highest bidder to be exploited.

- Amazon.com famously remotely deleted George Orwell's book 1984 from its customers' Kindle readers without users' consent.[8] Digital tracking and use of consumers' reading materials and records is an issue that will have to be tackled. Protecting the sanctity of book and reading material privacy is a current point of contention and discussion connected with e-books and e-readers such as Kindle, the Google Book settlement, and in other venues.[9]

- Teenaged girls who were active on Facebook were denied insurance for anorexia. When the parents sued the insurer, the insurer went to court and demanded the teens' Facebook pages, among other things. The lawsuit was eventually settled in the plaintiffs favor.[10]

- How many Cox digital phone subscribers know that Cox is analyzing and datamining subscriber phone calls made through the Cox system and assigning a "churn" (turnover of customers) prediction to them based on the characteristics of the people or phone numbers they call? Few if any consumers expect their actual calling patterns to be analyzed in this way.[11] A datamining vendor that Cox uses, KXEN, stated in a white paper: "Cox Communications started using KXEN in September 2002 in its marketing department to analyze its customer data base. It now produces hundreds of models for marketing campaigns in 26 regional markets from a data base of 10 million customers and 800 variables.[12] Most people understand that when they sign up with a company, the company does have access to increased amount of data about them. But analyzing customer phone call patterns for further marketing purposes and behavior prediction is something I would argue that most people are not expecting.

---

[8] Brad Stone, *Amazon erases Orwell books from Kindle devices,* New York Times, July 17, 2009. <http://www.nytimes.com/2009/07/18/technology/companies/18amazon.html?_r=1>.

[9] See for example EPIC, Google Books Settlement and Privacy. <http://epic.org/privacy/googlebooks/default.html>,

[10] Mark Stein, *Facebook page or Exhibit A in Court*? Portfolio.com, Feb. 5, 2008. <http://www.portfolio.com/views/blogs/daily-brief/2008/02/05/facebook-page-or-exhibit-a-in-court/>. See also Mary Pat Gallagher, MySpace, Facebook Pages Called Key to Dispute Over Insurance Coverage for Eating Disorders, New Jersey Law Journal <http://www.insuranceheadlines.com/pdf/4479.html>.

[11] Direct Marketing Association 09 Conference and Exhibition Presentation, *Automated Predictive Modeling: Cox Communications Shows It's Possible*, October 20, 2009, San Diego, California. Presentation abstract: "Can you imagine being able to refresh, validate and deploy your cross-sell and retention models every month? For 20 separate regions of the country, and 19 different products? Cox Communications will explain how they do this with KXEN. Now they can focus on the business, not the models." < http://mydma09.bdmetrics.com/SOW-2820200/Automated-Predictive-Modeling-Cox-Communications-Shows-It-s-Possible/Overview.aspx>. See also DMA 2009 Program, <http://www.dma09.org/>.

[12] KXEN, *Making More Decisions Intentionally and Competing on Analytics in the Real World*, KXEN White Paper < www.wgsystems.com.br/kxen/pdf/KXEN_extreme_data_mining.pdf> last accessed Nov. 17, 2009. KXEN is a data mining automation company.

- Consumers who walk into a store may not realize that their reactions and interactions with certain products in the store may have been recorded for marketing and profiling use. Two examples of this are gaze tracking and pathway tracking. When retail stores track consumer movements through the store, this is called *pathway tracking*. When digital signage displays track numbers of consumers who have passed the sign, who looked at the screen, and for how long, that is called *gaze tracking*. A retail expert discussed her concerns with the uses of these two shopper profiling technologies:

  > "During the course of 2009, we have seen more retailers utilizing **shopper path tracking** and **gaze tracking** to better understand how shoppers are responding to in-store promotions (both traditional and digitally-based). **As these technology tools become more prevalent, we have seen some retailers use them responsibly and others use them to track age, race and gender with the intent to eventually serve up 'targeted' messages to shoppers**. This raises potential privacy concern and, until we get in front of them, retailers are looking for new methods to stimulate shopper 'opt-in' to their targeted in-store promotions.[13] (*Emphasis mine*).
  >
  > The industry is debating this profiling issue, with some saying that it is sufficient to notify consumers of the profiling with a sign stating that the store is using video surveillance. Others are arguing for more privacy protections.[14]

- In the realm of online consumer data collection, consumer behavior is tracked via well-established techniques such as long-term tracking cookies, Flash cookies, web browser cache cookies, web bugs or "pixel gifs" and other techniques. I discussed these techniques in a detailed analysis of the effectiveness of the Network Advertising Initiative self-regulatory program in terms of consumer protection, and incorporate that material by reference here.[15] It is tempting to place online behavioral targeting in a separate category and look at it as a separate activity. But that approach excludes the importance of the other robust data sources. A more balanced way of approaching online behavioral advertising is to understand it as one aspect of the consumer data collection picture. It is closing the circle on consumer monitoring, but it has come at the end of a long chain of other consumer data collection activities, and often operates in conjunction with those activities.

A significant segment of our modern data infrastructure began in earnest with credit reporting, which managed to overcome the costs of data collection in a pre-computerized world because of

---

[13] Laura Davis-Taylor, *2-D Barcodes present path to get shoppers to "opt-in" to in-store*, Retail Touch Points, August 6, 2009. < http://www.retailtouchpoints.com/in-store-insights/295-retail-technology-trends-2-d-barcodes-for-shopper-opt-in-.html>.

[14] Laura Davis-Taylor, *The in-store shopper profiling debate*, May 20, 2008, POPAI Digital Signage Blog. < http://www.popaidigitalblog.com/blog/articles/The_in_store_shopper_profiling_debate-439.html>.

[15] Dixon, Pam. World Privacy Forum, *The Network Advertising Initiative: Failing at Consumer Protection and at Self-Regulation*, Nov. 2, 2007. < http://www.worldprivacyforum.org/pdf/WPF_NAI_report_Nov2_2007fs.pdf>.

the economic incentives. The development of later styles of consumer non-credit profiling activities, with lower value, was possible only because the costs of data collection were reduced by advances in technology.

The final step, also supported by low-cost technologies, is the near-pervasive consumer data collection and monitoring that is made possible by the merging, linking and analysis of a variety of offline and online data. This will lead to a completely new kind of detailed, *modern permanent record* kept on individual consumers. Even the most information-conscious, privacy-sensitive consumer cannot escape being profiled.

The result of this sort of pervasive tracking and *modern permanent record* creation, if it is allowed to occur, will be the creation of the most detailed profiles yet on individuals, with great impact on peoples' opportunities. Individuals who land on lists or databases with pejorative categorizations may find themselves excluded from opportunities. Those on the mental health marketing list – what opportunities have they lost? What has happened to them because of their inclusion on the list? We know what happened to at least one elderly veteran when he was included on a marketing list that identified him as an elderly opportunity seeker.

Other types of offline consumer monitoring, such as RFID, video surveillance, face recognition, cell phone tracking, and traffic monitoring are also dropping in cost. In the service of better, more efficient advertising, future consumer profiles and databases will use multiple sources of information in addition to "online" information. The additional data can include geo-location information, products that a consumer touched in a supermarket or retail store, retail items purchased in-person, and various business transactions such as activating a credit card. Commercial companies have no incentive to discard data. The costs of storage may be less than the costs of deletion.

Databases of consumer identities, demographics, transactions, and behaviors attract secondary users, and this is especially the case as the database compilers seek to find new sources of revenue. Secondary users will include government law enforcement at all levels, employers, insurance companies, schools, public health authorities, litigants, landlords, parents, stalkers, and others. The information – like credit reports – will be used to make basic decisions about the ability of individual to travel, participate in the economy, find opportunities, find places to live, purchase goods and services, and make judgments about the importance, worthiness, and interests of individuals. The information will also be used to predict consumer behavior. Under current law, this can happen without the knowledge or participation of consumers. Secondary use of unregulated, non-credit consumer information is already commonplace without any consumer awareness, with the government being perhaps a disturbingly large customer for the data.

Consumers are already being denied goods and services due to database profiles stored about them.[16] But politicians and government workers may be particularly vulnerable to the reputational aspects of increased consumer profiling. Imagine what a confirmation hearing for a Supreme Court Justice might be like in a few years, when the record of the nominee's "lifetime Web activities" or complete Web search history or Experian Consumer Database File is demanded by the Senate. Will there be a day when a casual or accidental click may prevent

[16] See <http://www.badcustomer.com>.

anyone from fulfilling his or her personal ambitions? Will there be a day when a consumer database or combination of consumer transactional databases are used to create a compilation of facts for an opposition ad on someone running for office?

The modern permanent record will be compiled from multiple sources both online and offline, and will impact any individual who is living a modern life. It will be largely unavoidable under current law.

II. Consumer Expectations of Privacy and the Cold Reality of Data Broker Activities

Consumers go about their daily lives with certain expectations of how information about them will be collected, stored, used and disseminated. Consumers' expectations of privacy in regards to their information and transactions are legitimate, but what consumers think is happening to their information is far removed from the reality of current business practices.

Over the years, I have watched as databases filled with consumer information gleaned from offline and online sources have been compiled, exchanged, sold, and stitched together. Marketing has changed with the times, and has become extraordinarily sophisticated. There is a good deal of focus at the Federal Trade Commission and in Congress on the use of consumer information in online behaviorally targeted advertising. There are legitimate reasons for concern in this area. However, it must be said that online behavioral advertising is just one aspect of an entire complex of consumer data collection, exchange, use, and reuse. The universe of this challenging consumer privacy issue is large indeed, and is relatively untouched by any meaningful regulation of any sort.

At the 2009 Direct Marketing Association annual meeting this October, vendors and practitioners discussed the latest advances in real-time consumer tracking, micro-targeting to the individual, and data appending, with plentiful examples. Of note was the persistent emphasis of merging online and offline information sources.[17] Also of note was a strong emphasis on predicting consumer behavior based on past behavior, or even on known relationships with other businesses or other consumers. The discussions at this event generally typify the industry trends.

In the past, marketers focused on acquiring certain discrete pieces of information about the customer. For example, acquiring the age, gender, ethnicity, etc. of a customer was a prime goal. But now, as discussed earlier, demographic information is just the beginning. Transactional information tied to individual consumers, sliced and diced into scores and predictions, that is the newer model. I would like to discuss some of these new approaches in more detail.

A marketing list called Consumer TransactionBase had this to say about why a list of 77 million-plus consumers was so valuable:

> Transactional data can be leveraged by direct marketers to gain powerful insight into a

---

[17] See for example the online optimization track <http://www.dma09.org/attendees/conference/Online.php?PHPSESSID=a3a74c1e2658569a8b6ea3333679edd3> and trigger marketing <http://www.dma09.org/attendees/conference/Trigger.php?PHPSESSID=a3a74c1e2658569a8b6ea3333679edd3> in the program.

household's needs and wants. **Through the examination of past spending patterns, marketers are able to analyze and predict future purchasing behaviors.**

Consumer TransactionBase compiles SKU-level transactional data from a variety of online and offline retailers to offer a complete view of economically active purchasing households. Additional uses for this detailed data set include modeling and analytics as well as data enhancement.

Major applications include:

Book and Magazine Subscriptions
Club Memberships
Donation Requests
Financial Products and Services
Lifestyle and Interest-Specific Offers
Personal Services
Store Announcements
Travel Offers

The Consumer TransactionBase file is updated quarterly. **Compilation comes from a leading nationwide cooperative database of consumer purchasing activity**. Company and industry usage restrictions may apply.[18] (*Emphasis ours*)

What does all of this mean to consumers? If consumers simply go about their daily lives, are cautious with their information, careful with who sees their Social Security Number, shred their bills and pre-approved credit card offers, use safe computing practices, and so forth, they will still have detailed information about their private and in some cases professional lives collected, bundled, bought, trade, sold, compiled, layered, appended, and in general, used in various ways to target or to deny goods, services, and opportunities.

Right now, consumers do not generally know what is happening to them, and if they did, they do not have sufficient rights to manage the information marketplace they find themselves in. Regardless of how cautious and informationally careful a consumer is, he does not have the ability to live a modern life and avoid being systemically profiled. Consumer profiling is currently unavoidable by the majority of consumers. I believe this truly defies consumer expectations of privacy.

The sheer volume of profiling data already being exchanged about consumers can be seen in the Experian Consumer Database. This database contains approximately 215 million consumers in 110 million living units nationwide.

The data card (or sales card) for the list states:

---

[18] Consumer TransactionBase, <http://listfinder.directmag.com/market;jsessionid=D111DD2A12B5CAE409CBCBE160539072?page=research/datacard&id=267942> last accessed November 6, 2009.

> **Target people by exact age, gender, estimated income, marital status, dwelling type, families with children, telephone numbers and a variety of other selections. The vast quantity of names on this database and its varied selection capabilities make this one of the largest and most flexible lists on the market today.**

The data card additionally states in regards to **predictive targeting**:

> Experian's Quick Predict[SM] modeling process is designed for marketers with small to medium-size customer databases that are looking for a cost-effective modeling solution. Quick Predict gives you fast results for acquisition, retention and cross-sell campaigns and to enhance your market research efforts. of current customers. We run acquisition models against Experian's extensive consumer data resources, providing you with a steady stream of potential new customers.
>
> **Quick Predict segmentation uses either customer surveys, market research or observed behaviors of your existing customers to create specific propensities (or scores) based on your own objectives.** The Quick Predict process matches your file to the INSOURCE[SM] Database to determine households that behave like your target customers.[19]

This is not the staid marketing list in use in years past – this is a list that is flexible, is used to create scores that predict consumer behavior, and is used to characterize consumers and put them in boxes of how they are predicted to behave. Opportunities and services are then offered to the consumers to match their *modern permanent record.* At what point does the contents of a *modern permanent record* accumulated through web links clicked, Facebook surveys, Twitter streams, sweepstakes, loyalty card programs, and the like become a person's destiny?

To take a different concrete example of a data collection that most everyone can identify with, customers at retail stores who are asked for their zip code do not understand that the zip code they are offering leads to a universe of additional new information about them. This practice of "data appending" in the retail environment is a significant point of data collection. While the zip code may be acquired at the retail cash register, that zip code can be and in some cases is merged with substantial amounts of other information, including information from other databases, which may include offline and online information. A recent court case has exposed the facts about how the inner workings of this occurs.[20]

This sort of data activity – prediction, analysis, data appending -- is often trivialized by those using the data. One frequently encountered argument is that this data activity is fine, because consumers want better ads, products, and services. **But there is no good empirical proof that consumers want an entire modern permanent record created in order to get a better ad.** Beyond that, it is crucial to understand that this profiling is not just being used to offer services and goods; it is also used to deny consumers opportunities, products and services. This is

---

[19] *Experian Consumer Database*, Nextmark ID 84312, Last accessed Nov. 6, 2009. <http://listfinder.directmag.com/market;jsessionid=749F1DAB78232862B6E4A48F4C9A7120?page=research/datacard&id=84312>.

[20] See Pineda v. Williams-Sonoma Stores, Inc., Cal. Ct. App., 4th Dist., No. D054355, certified for publication 10/23/09.

especially problematic when predictive analysis based on transactional data is used to categorize consumers in a negative way.

Note for example, the database of consumers who have disputed charges on their bills; certain of these customers are put into a database that is marketed as **"Badcustomer." This is modern permanent recordkeeping at its worst. The badcustomer.com web site states: "Are your purchasing transactions being denied? Find out if you've been blacklisted before it's too late."**[21] Consider the consequences of this database for identity theft victims -- these are individuals who *have to* dispute charges. Are they in this database? What services, goods, and opportunities will victims of identity theft be denied because they are in this database? How many lists like this exist that consumers don't know anything about?

I also note that to get off the Badcustomer list, consumers must supply detailed information online. How are consumers supposed to learn about databases like this? How is Badcustomers.com using the consumers' information after receiving it? Is this company doing more than just taking people off of the bad customer list?

I suggest that consumer data collection is out of control, with no balancing consumer rights or requirements for transparency to counterweight the collection and usage activity. As I will discuss in this testimony, I believe the institution of a rights-based approach that combines Fair Credit Reporting Act-like rights with additional Fair Information Practices rights will address this lack of balance.

Most consumers would be appalled to discover the ways their modern permanent record contains categories that describe them and circumscribe and determine their opportunities. For example, on a recent search I found 18,684 marketing lists containing the keyword "bad credit." I found 414 marketing lists containing the keyword "impulse." I found 1,282 marketing lists containing the key word "mental problems."

As seen earlier, these marketing lists contain names of millions upon millions of consumers, along with typically their name, age, gender, income, state, and a great deal of other detailed demographic information. Some lists also contain transactional information and merged information. These lists exist outside of most regulatory structures. Many consumers often have a vague idea that HIPAA will protect their health information no matter where that information exists. These consumers would be horrified to learn that it is not unusual whatsoever to find highly sensitive health information offered up for sale in these lists.

I have already shown you the MedNet Mental Health Problems list. Many of the consumers named on this list are not likely to know they are on the list. I also think that many of the consumers named on this list would welcome the option to delete their names and identifying information from this list, which is marketed with this pitch:

In this list, the data card (a form of "sales pitch" for the list) states:

---

[21] <https://www.badcustomer.com/blacklist.htm>. Last accessed November 6, 2009.

> "Mental health problems can create a significant burden on the afflicted individual, making them extremely receptive to any campaign that may be able to offer some assistance or relief."[22]

Returning to the issue of targeted marketing and how consumers purportedly like it, it is unlikely that the caretaker of an autistic adult would be happy to know that she is being targeted because she will be "extremely receptive" to certain types of campaigns.

I also think that some of the 6 million people on the Credit Card Declines marketing list would like to know they are on a list of people who have been declined for major bank cards, and would like the opportunity to delete their age, the age of their children, the gender of their child, dwelling type, ethnicity, and other information from the list and databases associated with it.[23] How does being on this list impact their modern permanent record?

There is an industry argument that consumers land on these lists and in these databases because they have given up their information freely. This may have been true at one time, but it no longer holds universally true. Consumers can get on these lists from freely giving up their information. But they can also get on these lists just from making a wrong stray click on a web site, opening a phishing email by mistake, or even by just conducting their lives. Even the most informationally careful consumer can land on these lists. This completely defies consumers' expectations of privacy and of fair play.

One example of this is the **Passport to Credit – Newly Activated Credit Cards** list. This list of 18 million consumers is sourced from a credit card transaction processor.

> This dynamic database is sourced from a credit card transaction processor, not from the source who issues the cards. You can select change of address, number of transactions, number of credit cards, type of credit card and more![24]

To stay off of this list, a consumer would have to not activate their credit card. How is that a reasonable choice?

Some lists and databases are an assault on the dignity of the people named in the list. One list, Fat Burner II, targets obese and morbidly obese consumers. The data card states: "These weight watching consumers will try anything in hopes of being healthy."[25] Another list, Free to Me – Impulse Buyers, is targeted to people who made recent online purchases because they received something free with their purchase. The data card states: "Free To Me – Impulse Buyers are very quick to respond to offers that come in the form of contests, sweepstakes, or other free products and services."[26]

---

[22] *MedNet Mental Health Problems*, Nextmark ID 233893.
<http://listfinder.directmag.com/market?page=research/datacard&id=233893>.
[23] *Credit Card Declines*, Nextmark ID 138236, last accessed November 6, 2009.
[24] *Passport to Credit – Newly Activated Credit Cards*, Nextmark ID 257747, last accessed Nov. 6, 2009.
[25] *Fat Burner II*, Nextmark ID 206453, last accessed November 6, 2009.
[26] *Free To Me – Impulse Buyers*, Nextmark ID 271702, last accessed November 6, 2009.

Loyalty cards, warrantee cards, sweepstakes, and many more items in this realm create a raft of information that flows into the *modern permanent record.*[27] Online information also flows into the *modern permanent record.*[28] As *modern permanent records* become an important influence on consumers' opportunities, much like the credit score did, consumers will need new rights to manage the situation they find themselves in.

III. The FCRA Model and Offline/Online Privacy

Perhaps the most successful -- but not perfect -- privacy law of longstanding is the Fair Credit Reporting Act (FCRA). Congress passed the FCRA after years of persistence by a Senator who understood (1) the essential importance of credit reports in the lives of consumers and in the operation of the economy, and (2) the lack of any rights or due process for consumers in the credit reporting system.

The activities regulated under the FCRA are absent from my discussion of consumer harms, because the regulations have been largely effective. **Commercial data brokers do not want to fall under the FCRA compliance regime, and many avoid FCRA activities as a result. They avoid knowing how their information is used in the real world.**

What is needed is a fresh look at the ideas contained in the FCRA and how its principles could be used to create variegated rules for the modern online/offline information environment. When information – whether demographic, online, behavioral, pictorial, or etc. might affect a consumer's rights, benefits, privileges, or opportunities in government, commercial space, or on the Internet, there should be some rules of the road that prevent consumer harms and give consumers rights. ***Modern permanent records* should be subject to rules.**

Some ideas:

- Some harmful collection and data storage activities should be banned altogether. For example, forms of redlining that would be impermissible in the analog world should also be impermissible in the digital world.

- Other consumer data compilation and use activities should have disposal requirements, much stricter than the seven years allowed under the FCRA.

- The compilation of some categories of sensitive information should be allowed only with the affirmative, time-limited consent of the data subject. Examples include medical and financial information, for example.

---

[27] See Givens, Beth, Privacy Rights Clearinghouse, *The Information Marketplace: Merging and Exchanging Consumer Data* , April 30, 2001 for further discussion of these issues. < http://www.privacyrights.org/ar/ftc-info_mktpl.htm>.

[28] See for example Rapleaf <http://www.rapleaf.com>. Rapleaf is promising to use consumer data gleaned from Twitter and other social networks to predict credit risk. This activity is broadly termed "Social Media Monitoring" or SMM. See Conley, Lucas, *How Rapleaf is Data Mining Your Friend Lists to Predict Your Credit Risk,* FastCompany, Nov. 16, 2009. < http://www.fastcompany.com/blog/lucas-conley/advertising-branding-and-marketing/company-we-keep>.

- Individuals should have the right to stop harmful dossier activity and to force the permanent and immediate expungement of all data that is factually incorrect, data that arrives at an incorrect conclusion about them, or data that influences decisions about a consumer in a negative way.

- Modern permanent records associated with an individual should be banned for anyone under the age of 16, and all pre-existing dossiers on individuals should be expunged when they reach the age of majority.

- Consumers should have a right to see and change their modern permanent records at no cost.

The legislation needed to implement these ideas will be quite complex, will require long-term discussions from all stakeholders. None of this will be easy. However, what is most important is that we recognize the stakes in the current limited public debate about online behavioral ad targeting. **Discussions that focus solely on consumer opt in and opt out in the online environment miss the point of the modern information environment: a consumer could opt out of everything online, but that would not have a substantive impact, because the digitization of our lives is profoundly more complete than that already.** And the uses of that information are already in place, and will only increase in scope.

The issue that a democratic society must debate is whether the prize here – completely unregulated use of consumer data for slightly more efficient advertising or marketing – is worth the full cost and the consequences. Mild-mannered limitations on behavioral targeting that some are considering at present will not be enough to head off the deeper problems that loom. Consumers need substantive control over their data. Consumers need to know about their own modern permanent records and to be able to mitigate its impacts on their lives. We need to look further down the road and build appropriate protections.

The stakes here are far greater than Internet advertising or the current model for Internet services. We need to remember what was happening with credit reports before the FCRA. In a similar manner, online and other forms of digital tracking will record the tiniest details, and these details will be used to control, shape, and affect consumer activities in subtle and not-so-subtle ways. This is what happened with credit reports, which have found other uses in spite of regulation.[29]

The importance of non-credit related consumer profiles in our lives will exceed the importance of credit reports if the non-credit profiles remain completely unrestricted. We need to develop regulatory protections that will place limits on these activities before these practices become cheaper and even more entrenched in business practices.

IV. Privacy Standards

---

[29] For example, the credit scoring phenomenon. See Hendricks, Evan. Credit Scores and Credit Reports, How the System Really Works, What you Can Do, 3rd edition. Atlas Books.

We have a good set of information privacy standards that were created originally in the United States, that have been blessed in U.S. and foreign legislation, and that are perfectly adaptable for present purposes. Those standards are Fair Information Practices (FIPs). For a short history of FIPs, see Robert Gellman, *Fair Information Practices: A Basic History*.[30]

The version of FIPs from the Organisation for Economic Cooperative and Development represents the gold standard of information privacy principles.[31] The eight principles set out by the OECD are:

> Collection Limitation Principle
>
> There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
>
> Data Quality Principle
>
> Personal data should be relevant to the purposes for which they are to be used and, to the extent necessary for those purposes, should be accurate, complete, and kept up-to-date.
>
> Purpose Specification Principle
>
> The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
>
> Use Limitation Principle
>
> Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with [the Purpose Specification Principle] except: a) with the consent of the data subject; or b) by the authority of law.
>
> Security Safeguards Principle

---

[30] Robert Gellman, *Fair Information Practices: A Basic History* <http://bobgellman.com/rg-docs/rg-FIPshistory.pdf>.

[31] < http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html>. There are equivalent statements from the Council of Europe and from the Canadian Standards Association, but the differences are minor. The Privacy Office at the Department of Homeland Security in 2008 issued its own Fair Information Practice Principles that that match closely the OECD version. Privacy Policy Guidance Memorandum (2008) (Memorandum Number 2008-1), <http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf>. The DHS issuance is noteworthy since it implements the first statutory reference to fair information practices in U.S. law.

> Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.
>
> Openness Principle
>
> There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.
>
> Individual Participation Principle
>
> An individual should have the right: a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; b) to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him; c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.
>
> Accountability Principle
>
> A data controller should be accountable for complying with measures, which give effect to the principles stated above.

In 2000, the Federal Trade Commission issued its own incomplete version of FIPs.[32] That statement of FIPs appears to have been abandoned, and it should not be revived. We see no reason to deviate from the FIPs principles in general use around the world.

To be sure, the OECD version of FIPs principles may not be perfect. There may be a need to consider, for example, whether there should be a principle addressing anonymity or pseudonymity. Nevertheless, the principles as they exist today are broad enough and general enough for the purpose.

V. Conclusion

In this testimony, I have discussed the *modern permanent record*, business practices in the online and offline world, and how online and offline data is being merged and linked. I have given concrete examples of current practices already in place. Why does any of this matter? **The online**

---

[32] Federal Trade Commission, *Privacy Online: Fair Information Practices in the Electronic Marketplace*, (May 2000), http://www.ftc.gov/reports/privacy2000/privacy2000.pdf.

and offline data collection of consumer data matters because it impacts all of our lives profoundly whether we know it or not.

Yes, there are benefits. But there are harms. But the most important idea I would like to convey to you is that information collection and use today is already robust enough and rich enough to influence what a person's world looks like to them. **Two people going to one web site or one retail store could already be offered entirely different opportunities, services, or benefits based on their modern permanent record comprised of the previous demographic, behavioral, transactional, and associational information accrued about them.** These same two people can also be subject to a denial of opportunities, services or benefits based on analysis of the same information.

It is still possible to avoid an environment where our demographic characteristics analyzed in combination with our online and offline activities (links clicked, people emailed, friends or businesses associated with) will be judged by a merchant, credit grantor, employer, insurance company, landlord, etc. to make a decision or a prediction about us. Do we want to live in a world where every small choice we make -- from who to call, what store to window shop, what street to drive down, who to friend, what to order for lunch -- will be weighed and assessed and possibly used in our lives? **Do we want to arrive at a point where people hesitate to buy things, go places, or even use the Internet lest it all be recorded in their modern permanent record maintained by some unknown company and over which they have no rights?**

Thank you for your attention to these matters. I welcome your questions, and will be happy to provide further research or input.

Mr. BOUCHER. Well, thank you very much, Ms. Dixon, and the committee's thanks to all of our witnesses for your informative testimony today.

I am going to ask a brief question, and I would appreciate a brief answer. And I will ask each of you just to respond to this in perhaps 15 seconds or less.

Assuming that we adopt a set of new privacy protections, should we apply those both with regard to online and offline transactions? Ms. Dixon.

Ms. DIXON. Yes, I believe you should, because the offline collection of data is highly identifiable, and it can include biometric information, name, health information, and other information that is entirely unregulated.

Mr. BOUCHER. Thank you. Ms. Bougie.

Ms. BOUGIE. I would say it can't be a one size fits all. Online information is different in many cases than offline, and so, I would recommend that we just be very cautious, because in the case of the small business, it would really restrict our ability ultimately to prospect with web searches and things like that.

Mr. BOUCHER. So, you are not saying apply it online only, you are just saying be careful about how you apply it to both.

Ms. BOUGIE. Be very careful, because again, the unintended consequences of what——

Mr. BOUCHER. I understand.

Ms. BOUGIE [continuing]. Would happen.

Mr. BOUCHER. All right. Thank you. Ms. Strickland.

Ms. STRICKLAND. Yes. Walmart does favor a principle-based approach that doesn't focus on one particular technology, and I think it is very hard to draw a line that clearly separates online from offline.

A lot of services now are both online and offline, so I think a broader view is needed.

Mr. BOUCHER. OK. Ms. Barrett.

Ms. BARRETT. Yes, Chairman. I think the——

Mr. BOUCHER. Microphone, please.

Ms. BARRETT. Can you hear me now?

Mr. BOUCHER. Yes.

Ms. BARRETT. OK. Yes, we think it should be not limited to online, but a broader perspective, but I would echo my colleagues' remarks about some of the nuances regarding what is practical to do in an online world, and what is not practical, or might need to be dealt with differently in an offline world.

Mr. BOUCHER. All right. Thank you. Mr. Pappachen.

Mr. PAPPACHEN. I would agree with the tenor of the comments so far, that convergence, as we have seen, would dictate that we have a more broader application. The nuances of the application should be carefully observed, but a broader application is correct.

Mr. BOUCHER. OK. Mr. Hoofnagle.

Mr. HOOFNAGLE. I think the answer is, it depends. Offline data collection is a little different, and——

Mr. BOUCHER. Microphone closer, please.

Mr. HOOFNAGLE. My answer would be, it depends. It depends on the substantive protections built into the bill, and whether they are appropriate in the offline context.

Mr. BOUCHER. All right. Mr. Hoofnagle, let me pose my second question to you.

You have performed, and we are aware of your study, that as I understand it, finds that two-thirds of the American public does not favor the receipt by them of tailored advertising. And given the benefits of tailored advertising that many on our panel have stressed here today, what do you think we might be able to do, that could change that number, and persuade more people that not only is it not harmful, but perhaps even beneficial to the receipt of that advertising to receive it?

Mr. HOOFNAGLE. That is a great question, Mr. Chairman.

Mr. BOUCHER. And pull the microphone closer, please.

Mr. HOOFNAGLE. We were surprised by the answer that so many Americans say that they principally reject tailored advertised, and troubled by that result, because it is clear that tailored advertising does have advantages for consumers and for businesses.

But we think also that consumers might have a lot of anxiety around information collection. They might not want information collection in one context to follow them into another. So, for instance, the targeted ads that you get at home when you are using the Internet for personal purposes might, consumers might not want that to bleed over to how they use the computer in the workspace.

I think that if there is greater transparency and rules around data collection, it might change that number, and more people might——

Mr. BOUCHER. So, let me just cite an example. Let us suppose that we adopt a law that says that any entity that collect information from a customer, whether that collection be online or offline, provide to the customer a thorough description of what information is collected, a thorough description of how that information is used, and then provide an ability, through a series of opt-in and opt-out arrangements, depending on what the information is, and how it is used, for that customer to be able to control the use, or perhaps control the collection of the information itself.

If we provide that set of consumer guarantees, what do you think that might do to persuade more people that having information collected for the purpose of tailored advertising is, perhaps, advantageous to them, or at a minimum, have them be willing to acquiesce in it?

Mr. HOOFNAGLE. That is an interesting approach. I would point out that our survey shows that people already assume that there are opt-in standards in place. Americans assume that they have a right of confidentiality in the marketplace.

Mr. BOUCHER. So, they are making that assumption, even when two-thirds of them say they don't want the tailored advertising.

Mr. HOOFNAGLE. That is right, and they are——

Mr. BOUCHER. And if they knew the truth, that they really didn't have even the measure of control they think they do, that two-thirds number might even be higher is what you are saying.

Mr. HOOFNAGLE. I think that consumers have a lot of anxiety in this area, and that might be one of the reasons why they are expressing that level of objection.

My collaborator and I, Joseph Turow at the University of Pennsylvania, argued that notice and opt-out might not be the most optimal approach, because consumers do not read privacy notices. They already assume that protections are in place. Opt-out, too, can be problematic. We argued that policymakers——

Mr. BOUCHER. You mean opt-in can be problematic?

Mr. HOOFNAGLE. Opt-in can be manipulated as well, and in fact, we explicitly said that the right answer is not just to go to opt-in. We discussed the idea of there being mandatory retention ceilings, so that information would have to be deleted after a certain amount of time.

Mr. BOUCHER. After a certain period of time.

Mr. HOOFNAGLE. And that would allow targeted advertising, but it wouldn't allow kind of a permanent profile.

Mr. BOUCHER. Let us suppose, just for the sake of this question, that we do those things, and that we have retention limits, full disclosure, a set of opt-in and opt-out opportunities to control what happens, do you think that instills a greater amount of confidence in the American public that the online experience is secure, and to the extent that they are engaging in offline transactions, that they have more control over their privacy?

Mr. HOOFNAGLE. I think it would. It would——

Mr. BOUCHER. Do you think it might enhance commerce, if we did such a thing?

Mr. HOOFNAGLE. Yes, sir. I think it would be——

Mr. BOUCHER. All right. My time has expired.

Mr. HOOFNAGLE. OK.

Mr. BOUCHER. Thank you for your answers. Those are very helpful. Mr. Radanovich.

Mr. RADANOVICH. Thank you, Mr. Boucher. And appreciate the panel of witnesses. Earlier, in my opening testimony, I talked about, there was one point that, you know, people, about the delivery of a catalog to your doorstep, and I expounded on a little bit extemporaneously, because I remember in the past, where the holidays would come around, or an event would happen in my family, and all of a sudden, you don't have one magazine or a catalog, you have got 10 or 15. Incredibly frustrating.

And what was more frustrating was the hassle it was to get these people to shut it down, if that is, because I didn't want them, and it just didn't—and I know that my following question will not speak to the issue of the collecting of private data, but it does speak to the issue of a person's ability to control what happens in their home.

And so, I want to ask each member of the panel. You know, I don't want to interrupt free commerce and trade, and as long as the boundaries are proper, I think it is good. But I am all for, in a number of ways, making sure that a family's home, to be politically correct, is its castle, and that the people in their homes have as much ability to control what drops on their doorstep, what pops up on their video, you know, their computer screen and such.

Can you, is there anybody that can explain to me ways that the industry could look to provide people with, really, a lot of ease in their households, to be able to shut this stuff down if they want to? I mean, I have got to think, if I was the father of a new child,

I may or may not appreciate the fact that I got a hundred catalogs in there, on how to buy a baby crib, and want to shut it down. But if I shut it down, I might think oh, gosh, maybe I do want that information. I would like to see that control in the home.

Has anybody given any thought to how you can shut that down, or ways to make it easier to do that? And I will just open it up to the panel.

Ms. Barrett, if you would.

Ms. BARRETT. Yes. I would point to the new self-regulatory guidelines that the Direct Marketing Association put into place last year, where you can go to their Web site, and you can opt out from all marketing communications, or you can pick certain companies that you can, even if you have a customer relationship with that company, and say I don't want to receive marketing communications from you.

I think this is a big step in the right direction, and one that is probably not as well known as it ought to be.

Mr. RADANOVICH. And it is not as well known as it ought to be, if I heard that right.

Ms. BARRETT. Correct.

Mr. RADANOVICH. Correct. Yes. Ms. Dixon.

Ms. DIXON. Thank you very much. The self-regulatory approach has merit. The problem is, is that it is just the good companies that are following the rules that typically join the self-regulatory efforts. And they are always the ones who, you know, you call and they stop sending the catalogs.

It is the bad actors, and that is why I think that a broader approach could be very useful in really curtailing this.

Mr. RADANOVICH. A more regulatory approach.

Ms. DIXON. That is correct.

Mr. RADANOVICH. Yes.

Ms. DIXON. And I think that one of the things to look at is looking at some data rights that are not identical to the Fair Credit Reporting Act, because it would be extraordinarily complex to do, but look at that, and saying what can we learn from that statute and apply to this area? Is there a way that consumers could have a regular, you know, standardized way of finding out what lists they are on, and seeing that information, making sure it is accurate, seeing that it is not retained for the duration of their lives, and so on and so forth.

I think that that approach would require a lot of discussion and very serious thought, but has merit.

Mr. RADANOVICH. OK. Thank you. Ms. Bougie, I wanted to ask you a couple of questions. In your testimony, you mentioned the one size fits all approach to this whole thing. Do you have any suggestions on what appropriate regulation might be, then, if it is not one size fits all?

Ms. BOUGIE. Well, our concern for the one size fits all approach is that the business concerns of small business are, excuse me, sorry.

Mr. RADANOVICH. There you go.

Ms. BOUGIE. Our concern with the one size fits all approach is that business concerns of a small business are vastly different from

those of a large corporation. So, this narrow view would restrict us, with very few options.

The online options help, because it helps level the playing field. And if regulations restrict online behavior as an advertising option, or the ability to prospect or gain email addresses, we will be left basically, our list will slowly, slowly go away.

Mr. RADANOVICH. Right.

Ms. BOUGIE. But I believe by allowing voluntary privacy standards with marketing data to continue, and we focus on the regulations of financial and medical, that it is going to be more advantageous for small business, and allow technology to prosper as it should.

Mr. RADANOVICH. OK. Ms. Strickland.

Ms. STRICKLAND. Thank you very much. I also would like to echo her remarks about the one size fits all, and I think that is true, not just for small companies and large companies, but this debate we are having about online and offline as well. So, as we think about what appropriate notice is, that will be different on a Web site than, as you might imagine, in a store. You are not going to have the ability to have the depth and level of information in a store notice, necessarily.

So, as we think about how do we do a principle-based approach, how do we make it flexible enough that it will work in a variety of contexts, a variety of technology, and a variety of companies.

Mr. RADANOVICH. All right. Thank you.

Mr. PAPPACHEN. I would just add that, two things. One thing, consumer expectation with regard to medium should play a role when you are looking at the issue of notice and/or consent. The second thing is, I think businesses, who are in business because they are effective at communicating certain messages to consumers towards the ends that they want, should be involved in the process, towards the ends that we are looking at here.

Mr. RADANOVICH. All right. Thank you very much. Thank you. Thank you, Mr. Chair.

Mr. BOUCHER. Thank you, George. Mike.

Mr. DOYLE [presiding]. Ms. Barrett, I understand your company, Acxiom, has roughly 1,500 pieces of data on every American. So, I am a male, I live in Pittsburgh, I am 56 years old. That is three data points, three pieces of information about me. That means there is roughly 1,497 data points left.

So, just between you and me, what else do you know about me?

Ms. BARRETT. Good question, and I appreciate your asking it. When we talk about 1,500 potential data points, what we are referring to is the different possibilities of information we might have about an individual.

And to give you an example, we have over 600 different lifestyle and interest categories. No one has all 600 variables. I happen to like to bicycle and cook and read, so that is 3 out of 600 for me.

Mr. DOYLE. So, that is all part of the 1,500.

Ms. BARRETT. So, that is all part of the 1,500.

Mr. DOYLE. OK.

Ms. BARRETT. So, I would say an average person may have 20 or 30 or 40.

Mr. DOYLE. Let me ask you some more questions, and they are just simple yes or no answers. So, could you send me a statement with everything you know about me?

Ms. BARRETT. We offer access to the data. We have two kinds of data. We have data that we use for marketing, and data we use for identity management and risk decisions. And the answer to your question is yes, for the data in the risk decision category, and we will send you a summary of the data in the marketing category.

Mr. DOYLE. So, could I log onto your Web site and see what others know about me, and what you sell to other people about me?

Ms. BARRETT. No, we do not.

Mr. DOYLE. No, that is fine. No is fine. Can I log onto your Web site, or can you send me a letter telling me who you sold my information to?

Ms. BARRETT. I am sorry, who sold?

Mr. DOYLE. Who you sold my information to? Could you tell me who you sold my information to?

Ms. BARRETT. We do track all of the sales that we make.

Mr. DOYLE. But could you give me that information? If I wanted to know who you sold my information to.

Ms. BARRETT. We do not provide that information to consumers.

Mr. DOYLE. Thank you. Can I choose to delete certain information that you have about me if something is old or out of date, or doesn't apply to me anymore?

Ms. BARRETT. Yes.

Mr. DOYLE. And how would that process work? How would I go in there and do that?

Ms. BARRETT. You would contact us, and ask if it is the marketing data, you would ask for the data to be deleted, and actually, we will remove the entire record, if you wish. On the risk side of the house, you can do it element by element, and pick and choose the elements that you wish to have corrected.

Mr. DOYLE. Very good. So, I can be completely removed from your database if I want, every trace about me gone, if I just call you and say I want everything you have about me erased. I can do that?

Ms. BARRETT. You can do that for our marketing products. We do not allow you to erase or remove all the data from our risk products. Those are the ones, and identity management products. Those are the products that catch the bad guys, and we don't let the bad guys opt out of that data.

Mr. DOYLE. So, tell me, I am curious. Where do you get all the information you have about me? Where does it all come from? Where do you get it from?

Ms. BARRETT. It comes from three primary sources. The first is public records and publicly available information. The second is surveys that consumers fill out, and volunteer information about their interests and life.

Mr. DOYLE. Like warranty cards?

Ms. BARRETT. Warranty cards is just one small part. And the third category is information from companies that have a relationship with you, and have given you notice and choice about the fact that your data may be shared with another party, a third party like Acxiom.

Mr. DOYLE. So, do you sell medical or other sensitive information that is attached to personally identifiable information? Do you sell that?

Ms. BARRETT. We do not sell what we call sensitive information in any of our marketing products. Medical data, unless it is self-reported by the consumer, we would have no, personal health information is regulated by HIPAA in any of our marketing products.

Mr. DOYLE. What is the minimum information you need to identify someone? How many data points do you need to identify someone?

Ms. BARRETT. A name and address would be the baseline.

Mr. DOYLE. So, with two data points, you can pretty much identify anyone?

Ms. BARRETT. Well, we can, it depends on what we are using that information for. If we are using it for marketing, that may be sufficient to say we don't want to market to this person or we do.

If we are actually using data for an identity application, we would need more data points——

Mr. DOYLE. I see.

Ms. BARRETT [continuing]. To verify that you are who you really claim to be.

Mr. DOYLE. Tell me, do you audit the companies that buy the information from you? I mean, do you make sure they lock it up properly, that they use it for what they say they want to use it for?

Ms. BARRETT. For any company that buys any kind of sensitive data from us, we do both an onsite inspection, and an audit of their practices, to make sure that they are going to treat that information responsibly. For data, for companies that buy non-sensitive information from us, we go through a credentialing process, which makes us comfortable that that company is a legitimate entity, and that they will respect the terms of our contract, and keep the information confidential.

Mr. DOYLE. And our committee has had several hearings about data security and online security. Have you had any security breaches?

Ms. BARRETT. We had an incident back in 2003, where one of our external servers was hacked. And we used it to transport information back and forth between our clients. But fortunately, we had had a policy on that server that any sensitive information needed to be encrypted, and so, no consumers were put at risk as a result of that incident.

Mr. DOYLE. How would you inform a consumer whose information had been compromised? What would your procedure be?

Ms. BARRETT. Well, it would——

Mr. DOYLE. Or do you do it?

Ms. BARRETT. Well, it would depend on whose data the information was. If it was Acxiom's data, because we have both our own data products that we sell in the marketplace, and we also provide computer services for clients, who are hosting and housing their data on our computers. If it was Acxiom's data, we would be responsible for the notification. If it was client's data, we would work with that client, to make sure the consumers were notified.

Mr. DOYLE. Thank you. Just one final question, for Mr. Dixon and, I am sorry, Ms. Dixon and Mr. Hoofnagle. It is clear that vast

amounts of personal information about individual consumers are collected, aggregated, analyzed, and sold for a variety of commercial purposes.

In response, some people say so what. If a person likes to ski, but is mistakenly identified in the database as an angler, and received offers or coupons for fishing equipment, what is the harm? Ms. Barrett recommended, in her written testimony, that before we engage in additional regulation, we should articulate the extent of the harm.

So, I want to ask Ms. Dixon and Mr. Hoofnagle, can you please answer that question? Where is the harm to the consumers? And also, I want to give you a chance to maybe just react to my line of questioning to Ms. Barrett, and whether you have any thoughts on that. If you think this is what Americans expect, and what kind of rules of the road do you think we should put in place?

Mr. STEARNS. That is a lot of questions.

Mr. DOYLE. I know, and I am going to get to you, Cliff, and be mighty generous with your time. Go ahead.

Ms. DIXON. Thank you for your question.

A couple of thoughts. First, I want to talk about the harm, and then, I would like to respond to the line of questioning.

Mr. DOYLE. Yes.

Ms. DIXON. Your question. The one thing is that is quite clear is that the companies, when they discuss these issues, you will hear companies talk about the benefits of having this information available. And there is no question that there are benefits. I don't think anyone is arguing about the benefits. We know there are benefits.

The problem is, is that there are, indeed, also harms. So, for example, it is the shadow side of all of this. The same information, we saw it on badcustomers.com database, the same information that is used to target advertising is also used to deny transactions of consumers who have done, disputed charges.

So, you have the same information being used for completely different purposes. Once the information is compiled, you really lose the ability to determine how that information will be used, and in all the contexts that it will be used, unless it is covered under the Fair Credit Reporting Act. But what we have been talking about here today are all non-FCRA uses of the data, and also, all non-HIPAA uses of the data. So, it is really outside of regulation.

The second thing would be inaccuracies, outdated information, and again, incorrect inferences. I think that when you have these very clear pictures of consumers, you really do get locked into a bit of a pictorial box. Here is what consumer X or Y looks like. Here is how we are going to treat this consumer.

We are familiar with the situation where people were not allowed to vote because they landed in certain databases. Some of this information was incorrect. So, we are talking about substantive rights that can be impacted here. So, it is the picture of the consumer. Is this the right picture? If it is not, how do we correct that?

Mr. DOYLE. I am so far over my time. I am just going to ask Mr. Hoofnagle, for a quick response, and then we will get to the next witness.

Mr. HOOFNAGLE. I will be quick. I would turn the harm question around, and say, and ask retailers questions like why are they trying to re-identify consumers without telling them about it?

So, I detailed in my testimony the example of one company that will ask for your zip code at the register. If you give your zip code, they will combine it with your name from a credit card swipe, and then, they will go out and get your home address. Why not just ask the consumer can we have your home address? The fact that so much of this data collection occurs in secrecy, I think is, speaks to the harm issue.

Mr. DOYLE. Thank you very much. My time has long since expired, and I am going to yield now to my good friend from Florida, Mr. Stearns.

Mr. STEARNS. I thank you, Mr. Chairman. I just compliment you on your rapid fire questions. You got a lot of questions in there, and I am impressed.

I went to Drudge and I deleted all my cookies, and so, I came back the next day to go on Drudge, and it wouldn't go forward until it allowed me to put these cookies back on. I had to put on 17 cookies.

I went to the Gmail to do my Gmail, and I deleted all the cookies. Same thing happened there. So, that is an awful lot of cookies that I don't know what is going on, and this is for George Pappachen.

In your testimony, you mentioned the use of passive tracking technology, including cookies, in current studies. I guess your holding company is WPP, is that it? Yes. Use these passive tracking technologies. What do these tracking technologies do? I am a consumer. You are tracking my cookies. So, what are you looking for, and is the information you get useful, and what is it?

Mr. PAPPACHEN. Right.

Mr. STEARNS. Just pull the mic up a little closer.

Mr. PAPPACHEN. Sure. Passive tracking technologies can be utilized in different ways. A couple of the ones that I cited in my written testimony is, one, ad exposure, the fact that you were exposed to a certain ad.

Mr. STEARNS. Can you tell that from a cookie, that I was exposed to an ad?

Mr. PAPPACHEN. Yes, you can tell which ad you——

Mr. STEARNS. So, when I get an ad on Drudge for a car or for a book, that is based upon my previous search engines on Drudge or Google, and so, you get from those cookies, you read those cookies and say, OK, Stearns went to Amazon.com, he went to these sites and these sites. You find that all out.

Mr. PAPPACHEN. Right. Well, it wouldn't be as far as going to search, or there might be some categories where you might not have availability to track or know what the consumer engagement was, but there are, on a larger scale, there is the practice of tracking exposure to advertising, so that you are not burdened with excessive advertising of the same kind, or——

Mr. STEARNS. And you sell this to the advertisers to tell them, this is how effective you were or not?

Mr. PAPPACHEN. Right. So the idea is to understand how they performed, whether we are being relevant or not, similar to how we would do it with TV, or in another forum.

Mr. STEARNS. As a customer, do you make the customers aware of this? In other words, let us say you are doing this on me, how would I find out that you are doing it, and what you are doing?

Mr. PAPPACHEN. Sure. One thing we have been actively encouraging and working on is proactive privacy. The Privacy Icon project that we were involved in is about allowing for an enhanced notice to consumers. That then gives them disclosure.

Mr. STEARNS. But you are not now doing it.

Mr. PAPPACHEN. It is a self-regulatory initiative that is underway. We are definitely doing the best standards or best practices of informing about our practices within privacy policies and wherever else we can, but we are encouraging that the industry absorb an enhanced notice under a self-regulatory framework, that allows for disclosure that may be more relevant to them, that we were being told is important for consumers.

So, we are trying to respond in a way that allows for consumers to have transparency, but then allows for business to have, work in the way that it traditionally has, to be effective in their communications.

Mr. STEARNS. You know, we tried to pass a spyware bill here in the Energy and Commerce. We just couldn't get the Senate to agree. And within that spyware, there was a study that Mr. Dingell put in to look at cookies and the impact.

Do you think the privacy bill should have anything applicable to cookies that come into the computer?

Mr. PAPPACHEN. I think that, regulating technology is a tricky thing, as we have often heard.

Mr. STEARNS. That is what I mean, yes.

Mr. PAPPACHEN. I don't think technology is necessarily the enemy. I think we can talk about the uses of it. I think we can talk about how we disclose how we are using it. We can talk about how we give over the levers of control about how we can use it.

Mr. STEARNS. You said, you discussed a technology developed in 2007, one of your subsidiaries, Safecount, that allows users to see not only what tracking cookies are on their computer, but what data they are collecting, but also, where the tracking cookies came from. So is that in practice, that Safecount, is that being used?

Mr. PAPPACHEN. That is right. Consumers can have insight into what cookies there are on their browser, from Safecount, and also, which ad it was spawned from.

Mr. STEARNS. Has this Safecount program been given to other companies, besides WPP?

Mr. PAPPACHEN. It certainly could be. It is a, what I said in my written statement is that we have seen other, larger actors now going in that direction. It was in support of the idea that self-regulation can work.

We have seen other actors going towards providing access to the interests and profiles that they build online, and letting consumers have some control over whether those interests are built, and what those interest groups, they would want to belong to or not.

Mr. STEARNS. Do you think we should prevent spyware?

Mr. PAPPACHEN. I am sorry, sir. I didn't get the last part.

Mr. STEARNS. Do you think we should prevent spyware, in Congress?

Mr. PAPPACHEN. I think spyware by, again, it would matter what we define as spyware, but spyware, if it means something that consumers did not transparently get notice of and consent to, and it engages in activity that that would not want, yes, I think it should be prohibited.

Mr. STEARNS. OK. Ms. Barrett, Mr. Doyle talked to you about, he asked a series of questions, and he said will you tell me this information, and you said, we will not tell you information about risk product? Is that correct?

Ms. BARRETT. We will tell you. We will show you exactly what we have in our risk and identity management products, yes.

Mr. STEARNS. But he said, can I get all of it, and you said no, I thought.

Ms. BARRETT. For the marketing products?

Mr. STEARNS. Yes.

Ms. BARRETT. We offer a summary of the information, not the details.

Mr. STEARNS. And some of the information you won't provide, and why would that be? Because it is proprietary information that you have developed, that you have a proprietary interest in, is that, perhaps, why?

Ms. BARRETT. No, it is the fact that the information is not commonly requested at an individual level, and so, we have not put the systems in place to go retrieve it, and look at it on one person. Marketing applications look at the data in thousands or tens of thousands or millions of records at a time.

Mr. STEARNS. He had also asked a question about regulating online collection and use of data, should be clear about the extent of the harm we are seeking to address. Do you believe that harm exists in online data collection, or is it a risk of harm?

Ms. BARRETT. I think that there is the potential for harm in almost any data collection. I think it speaks to how do we use information, and where can we define risk under, in certain uses, and then, how can we develop guidelines that either prevent or mitigate against that risk, relative to that use?

And for example, I might point out some of the self-regulatory guidelines that have been put in place. For instance, for marketing, by the Direct Marketing Association and the Internet Advertising Bureau, and the Network Advertisers Initiative. Those are three different groups that have defined different kinds of guidelines, relative to different marketing activities.

Mr. STEARNS. This is the last question, Mr. Chairman. This is the more tough, you know, here we are trying to legislate a privacy bill. What harm should this privacy bill address, then? I mean, can you say that concisely?

Ms. BARRETT. Well, I think that is the challenge, is defining exactly what are the harms that——

Mr. STEARNS. Yes.

Ms. BARRETT [continuing]. Consumers are at risk of.

Mr. STEARNS. Yes.

Ms. BARRETT. My panelist down here, Ms. Dixon, mentioned some of the things, in terms of denying consumers substantive benefits, and I think that might be an area to explore. It is certainly not an area that we see in the marketing arena, but information that is used outside of simply trying to reach you with a relevant communication well might present some harms to the consumers. And those should be explored.

Mr. STEARNS. Thank you, Mr. Chairman.

Mr. DOYLE. Thank you, Mr. Stearns. The chair now recognizes Mr. Inslee.

Mr. INSLEE. Thank you, Mr. Hoofnagle. I was looking at a document attached, I think to your testimony from the Vente Company, which shows lists of, is this your information?

Mr. HOOFNAGLE. It is.

Mr. INSLEE. Yes. So, it shows this company, it appears that they sell lists of people who have certain conditions. So, cancer prostate, it shows they have 125,400 names of people who have cancer of the prostate.

Is that, do I read this right? This company will tell you who has cancer of the prostate?

Mr. HOOFNAGLE. I think you are referring to two different portions of my appendix here. One is the ailments, diseases, and illness sufferers mailing list, which is sold by a company that is a member of the Direct Marketing Association.

The Vente list is the addiction responders list, and it advertises who is struggling with an addiction to gambling, sex, or food. Who just can't say no to drugs, alcohol, or tobacco. Millions of America, and Vente has them.

Mr. INSLEE. So, Vente has the names of people who have had an alcohol problem, then, and they sell those names, is that right?

Mr. HOOFNAGLE. That is what their advertising claims.

Mr. INSLEE. And typically, where do they get the information that a person has had an alcohol problem?

Mr. HOOFNAGLE. The sources are likely to be self-reported. So, for instance, if a consumer fills out a survey, and checks a box saying that I have struggled with alcoholism, that is information that could be bundled and resold, in this type of context. It would not come, for instance, from a healthcare provider. So, this would be, it could be a product loyalty card, that is associated with purchases, or self-reported data.

Mr. INSLEE. So, let me ask you about the other document. Let us talk about cancer of the prostate. This other document suggests that there is a database of people suffering from a wide variety of ailments, diseases, illnesses, and medical conditions. Included are cancer of the prostate, there is 125,400 names, as I understand that.

Does this group sell names of people with that condition?

Mr. HOOFNAGLE. This information is personally identifiable. So, it is name and address, and then, if you look along the right hand side at the first page, there are what are known as selects, which means that for extra money, you can buy their age, ethnicity, sex, whether they are a homeowner, et cetera.

Mr. INSLEE. And where, typically, would this company have received the information, the personally identifiable information of the people who have cancer of the prostate?

Mr. HOOFNAGLE. With respect to this list, its provenance is claimed to be a lifestyle questionnaire. So, an example would be, you are walking through the mall and someone stops you and says, will you fill out this survey, and we will give you a gift card, or we will give you something free. If you fill out that survey, it could end up in a database like this, and there is no right to notice. They don't have to give you notice that they are selling the data. They don't have to give you access, et cetera.

Mr. INSLEE. So, they don't have to tell you that it could be used by someone who has got a grudge against you, and wants to publicly divulge that information to embarrass you, then.

Mr. HOOFNAGLE. That is really unlikely in this context?

Mr. INSLEE. Because?

Mr. HOOFNAGLE. This information is sold in bulk. If you look at the terms, it says $150/m, which means that it is 1,000 names for $150. You could not say to these companies, I would like to know whether Chris Hoofnagle is in the cancer list.

Mr. INSLEE. Why not? Why couldn't somebody say give me $10,000 and tell me all you got on Mike Doyle? Could they legally do that?

Mr. DOYLE. It wouldn't be worth that much money.

Mr. HOOFNAGLE. These companies are not set up to, at least this type of company, is not architected to sell information about a specific individual.

Now, with respect to the pizza delivery exhibit that I provided, where Merlin Data is selling identifiable information about people's homes, their unlisted phone numbers, their cell phone numbers, et cetera, that is very different. That is when you say, this is a situation where you say I want information about a specific individual. Do you have it?

Mr. INSLEE. Thank you. I believe, Ms. Barrett, you were Acxiom. Do I have, yes, I am sorry. So, you show a document, I am looking at the health buying activity, and they show various codes I am looking. Code 6437 is for health, female wellness. Code 6436 is health, diet/weight loss. What would be the information to generate people's inclusion in those codes? Where would you generate that information?

Ms. BARRETT. It would come from self-reported or survey information, where the consumer has indicated that they have an interest in information about that topic. And for the surveys that we use, we require that there be a notice that the information will be used for marketing purposes to other parties, and give the consumer the chance to opt out of that, or to come to directly to us, and say I don't want you to use that information.

Mr. INSLEE. So, if a person visited a Web site selling a weight loss product, could their visit to the Web site, to their opening that page, end up being coded on this in some fashion?

Ms. BARRETT. I don't believe so.

Mr. INSLEE. And what leads to a little question about that in your mind?

Ms. BARRETT. Well, I am not, I would have to go back and look at all the individual sources that contribute to that.

Mr. INSLEE. So, is there any legal, let me ask the panel in general. Is there any legal prohibition at the moment, if a person visits a weight loss Web site, that provides weight loss services or products. Let us say a person just visits the Web site, opens the page. Is there any legal prohibition of that owner of that page disseminating to a data information service the fact that this computer, this identified computer, has visited that site, and then that data collector, being able to collect, if they have some connection to an individual, connecting that to the data. Is there any legal prohibition on that happening right now?

Ms. BARRETT. There is no legal prohibition, but industry code or conduct, as well as the Direct Marketing Association Code, calls for the disclosure of that practice to the consumer, and at least in a privacy policy, if not more boldly on the page, and then, the chance for the consumer to opt out of that disclosure to another party.

Mr. INSLEE. Ms. Dixon, did you——

Ms. DIXON. Thank you. It is a good question. There is no legal requirement for that to happen. And one of the more troubling issues with Web sites is that they are very compelling. You can take, for example, Facebook surveys, where especially children, teens, and young adults will just go in, and they are very inured to giving out certain information, such as about anorexia and other, you know, topics they talk about online now.

They will give the information out, and these notices can be quite small, and they don't see them. And then, their information gets sold. So, it is not just that you visited a weight loss Web site. It is that you visited the site, then you filled out your name and, perhaps, gave them your email, and then, that can be further associated downstream, and used in collaboration and linked with other data.

But in some cases, the information is so identifiable, it doesn't even need to be linked. When you look at these really scary lists of ailments, you have prostate cancer, the mental health lists, these people are known by name, because they have freely given their name.

And one of the really difficult questions, I think, that this committee faces is that the opt-in opt-out model is very challenging, because it is so challenging to educate consumers about well, what does giving your name on such a Web site actually mean to you? Are you opting in? Do you really know what you are opting into? Because, for example, the mental health lists. Those people gave that information up in some way, typically, through some kind of Web site or survey or a sweepstakes. And did they really, truly know and comprehend the full consequences of their actions? It is a tough question.

Mr. INSLEE. Thank you very much.

Mr. DOYLE. Thank you, Mr. Inslee. The chair recognizes Mr. Rush.

Mr. RUSH. Thank you, Mr. Chairman. I just have some questions. I know that the time is quickly passing by, and I just have some questions for the panel. Now I, something that I will just ask Professor Hoofnagle about this, some questions.

Professor Hoofnagle, we don't need to look at any further than Acxiom's data products catalog or the Nextmark Web site referenced in your testimony, to see that companies are collecting and selling personal information about individuals, that many Americans consider sensitive, such as their race, ethnicity, religious affiliation, and political affiliation, not to mention information on a wide range of sensitive health topics and medical conditions, including addictions, sexual dysfunction, viral disorders, body odor, obesity, infertility, and menopause. This list can go on and on and on. A lot of sensitive information. Are any topics off limits for commercial use, or is the general rule that if information exists, collect and sell it?

The next question is, if we can agree that some categories of data should be off limits, or require heightened levels of consumer consent, how do we define that category of sensitive data?

Mr. HOOFNAGLE. Mr. Chairman, those are two very good questions. If I could address the second one first. I have tried to move away from the opt-in opt-out question, because framing rights in that way can easily be manipulated. It is easy to trick people into opting in, and conversely, it is easy to make it so people will not opt out.

So, I have suggested several other interventions. One is having the data disappear after a certain amount of time. So, if you have an upward data retention limit is one way of doing it. But there are other tools from the advertising world that can be used.

One example is advertiser liability. So, for instance, in the telemarketing, spam, and junk fax laws, advertisers can be liable if they hire spammers who, excuse me, advertisers can be liable if they send out, if they hire someone to send out email that violates the CAN-SPAM law.

In this context, you could create liability for people who buy certain lists and abuse them. An example out of Iowa is worth nothing. There was a list brokerage company there that was selling a list known as "elderly impulsive," and they were using it to take advantage of senior citizens who had problems remembering, and as a result, were able to architect a scam around that.

The data seller, I think, should offer some due diligence, especially when there are, using sensitive personal information. And that can be in reviewing the advertising that is ultimately disseminating, or in being responsible if the advertiser ultimately uses the information to take advantage of people.

You know, with respect to your first question, the general legal standard in the U.S. is that offline data collection is not regulated by a specific federal privacy law, except in certain areas. Your video rental records, for instance, are protected. Your cable records are protected. But between, in all the gaps left by the sectoral laws, there is data collection even on sensitive personal information.

Mr. RUSH. Thank you. I yield back.

Mr. DOYLE. Thank you. Well, seeing no more members here, we want to thank all of our witnesses for their testimony today, and this hearing is adjourned.

[Whereupon, at 3:00 p.m., the Subcommittees were adjourned.]

[Material submitted for inclusion in the record follows:]

Statement of the Honorable Joe Barton
Ranking Member, Committee on Energy and Commerce
"Exploring the Offline and Online Collection and Use of Consumer Information"
November 19, 2009

Thank you, Mr. Chairman, and thank you for holding this hearing.

I want to commend Chairman Boucher, Ranking Member Stearns, Chairman Rush, and Ranking Member Radanovich on their efforts this Congress to be leaders on privacy issues. Our committee has a long history of investigating these issues, and I'm glad we're continuing that work. I hope that we can apply that bipartisanship to any legislative solutions. Chairman Markey and I have shown that there need not be anything inherently Democratic or Republican about protecting people's privacy, and I know of nothing that would prevent us from sitting down at the same table to draft legislation if we decide that is what is needed.

Furthermore, I am pleased that Mr. Rush's Subcommittee and the Full Committee acted on the Republicans' original data security bill. We also moved legislation on peer-to-peer software that is a step forward in informing consumers about how to better protect their information and their personal computers. Both the peer-to-peer issue and the data security issue continue to appear in the headlines, and I'm hopeful we can move these bills to the suspension calendar, through the Senate, and to the President's desk.

Today's hearing is a little different than some others we have had recently about privacy. A lot of the media buzz in the technology and privacy communities has centered on online behavioral advertising or contextual advertising. As we all know, however, information collection and use is a much bigger discussion. We can't miss the offline forest while examining a few online trees. Spyware and online financial fraud are simply 21st-Century "dumpster diving." And we still have dumpsters. Online

targeting is simply 21st-Century direct mail. And we still have direct mail. There are online sites where you can access scores of public records from across the country. And yet we still have courthouses and town halls with file cabinets full of paper documents.

The relevant questions today are about how this brick-and-mortar world is being merged with its online counterpart. How are these new sets of data being used? How does it differ from the "old" use of this same information? Are consumers harmed in the marketplace? Are consumers well-informed about this collection of data? Do they have options to access the information that is collected? What options do they have to prevent collection and use?

Perhaps most important are questions and concerns about the sharing of this data. When I go into the Sports Authority store to buy a baseball glove, they know I'm there. And they know what

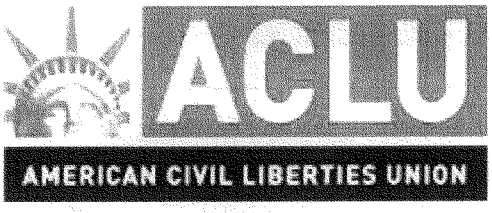
I've bought. I know they know, so I'm not going to be shocked to get a Sports Authority catalog perhaps a coupon for a Texas Rangers jersey in my mailbox. But if a retailer I visit sells information about me and my purchase to someone else without my consent, and that third party starts using the information to market to me, I going to be a little troubled. Magnify that by what happens when a giant company with many subsidiaries and helpful subcontractors, some of which may be very different kinds of business. When scores or hundreds of companies begin sharing information that was gleaned through a single transaction, I think many Americans get uncomfortable. And I'm one of them.

As most people know, I am the co-chair of the Congressional Privacy Caucus with Mr. Markey, so I have a long-running interest in this debate. Our responsibility is to find the consumer harm here, and that may not just be financial harm. Many consumers tell us that the mere unauthorized collection and sharing of this information is intrusive and harmful. Additionally, we need to get

an idea of the state of the regulation—and the state of self-regulation—in this area. If there is a lack of robust consumer education, if there is a lack of meaningful consumer choice, if there are holes in the system, we need to plug them.

I thank the panel of witnesses for travelling to be here and for their help in this discussion. I look forward to their testimony.

Thank you, Mr. Chairman, and I yield back.



Written Statement of the
American Civil Liberties Union

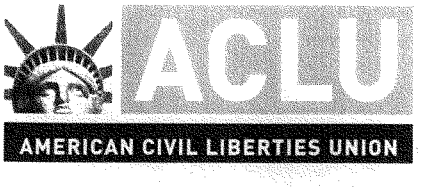
Michael W. Macleod-Ball
Acting Director, Washington Legislative Office

Christopher Calabrese
Legislative Counsel

before the
House Energy & Commerce Committee
Subcommittee on Communications, Technology & the Internet
&
Subcommittee on Commerce, Trade & Consumer Protection

November 19, 2009

Hearing on "Exploring the Offline and Online Collection and Use of Consumer Information"



WASHINGTON LEGISLATIVE OFFICE
915 15th Street, NW Washington, D.C. 20005
(202) 544-1681 Fax (202) 546-0738

Written Statement of the
American Civil Liberties Union
Michael Macleod-Ball
Acting Director, Washington Legislative Office
Christopher Calabrese
Legislative Counsel
before the
House Energy & Commerce Committee
Subcommittee on Communications, Technology & the Internet
&
Subcommittee on Commerce, Trade & Consumer Protection
November 19, 2009

Chairman Boucher, Chairman Rush, Ranking Member Stearns, Ranking Member Radanovich and Members of the Committee:

On behalf of the American Civil Liberties Union (ACLU), a nonpartisan public interest organization dedicated to protecting the constitutional rights of individuals, and its half million members, activists, and fifty-three affiliates nationwide, we congratulate you for turning your attention to behavioral marketing, a widespread and often intrusive practice of tracking and using information about the online behavior of consumers. As you consider this important issue we hope you will focus not just on private actors but also government use of information collected online. For all the reasons that the collection and use of this information is intrusive when performed by individual companies, it is all the more troubling when the information is disclosed to the government. Because the existing legal framework provides little meaningful protection against this surveillance, it is vital that new laws addressing behavioral marketing also regulate the disclosure of this information to the government.

I. The data collected by behavioral marketers forms a personal profile of unprecedented breadth and depth.

As much of the testimony before your committee has already made clear,[1] behavioral advertising involves the collection of a staggering amount of information

[1] *Behavioral Advertising: Industry Practices and Consumers' Expectations: Hearing before the H. Subcomm. on Communications, Technology and the Internet of the H. Comm. on Energy and Commerce, and the H. Subcomm. on Commerce, Trade, and Consumer Protection of the H. Comm. on Energy and Commerce*, 111th Cong. (2009) (Statement of Edward W. Felten, Professor of Computer Science and Public Affairs, Princeton University) *available at*

about people's online activities. At the outset this practice should be differentiated from "contextual advertising," another type of online ad service which shows ads to users based on the contents of the web page they are currently viewing or the web search they have just performed.[2] When this pairing of ads to users' interests is based only on a match between the content of an ad and a single page or search term, a website or advertising network requires no personal information about a user beyond an I.P address and the practice does not raise significant privacy concerns.[3]

As your committee hearings have demonstrated, behavioral marketers are far more ambitious and seek to form a much more complete picture of users. They do this by combining a vast amount of information gleaned from different web sites over time, including web page visits, searches, online purchases, videos watched, posts on social networking, and so on.[4] Any particular website may have little information, but when a large number of these data points are aggregated, the result is an extremely detailed picture.[5]

A striking recent development involves the potential to collect data from social networking sites like MySpace, Facebook, Twitter, and LinkedIn. A scholarly paper reports that eleven of twelve sites studied had the potential to "leak" personally identifiable information about users to third parties, including information such as name, address, phone number, gender, and birthday.[6] Approximately 90% of users did not take advantage of privacy controls to limit access by third parties, and those controls, when used, often proved ineffective against technically-savvy snoopers.[7] In the words of the Electronic Frontier Foundation, "The main theme of the paper is that when you log in to a social networking site, the social network includes advertising and tracking code in such a way that the 3rd party can see which account on the social network is yours. They can

---

http://energycommerce.house.gov/Press_111/20090618/testimony_felten.pdf (last visited October 7, 2009); *id.* (Statement of Jeff Chester, Executive Director, Center for Digital Democracy) *available at* http://energycommerce.house.gov/Press_111/20090618/testimony_chester.pdf (last visited October 7, 2009).

[2] Chester, *supra* n.1, at 3.

[3] *Id.*

[4] Felten, *supra* n.1 , at 3-4; CENTER FOR DIGITAL DEMOCRACY, ET AL., ONLINE BEHAVIORAL TRACKING AND TARGETING: LEGISLATIVE PRIMER 2009 3, *available at* http://www.uspirg.org/uploads/s6/9h/s69h7ytWnmbOJE-V2uGd4w/Online-Privacy---Legislative-Primer.pdf (last visited October 5, 2009); *see also* OMNITURE, THE RISE OF ONSITE BEHAVIORAL TARGETING 1 (May 2008) ("On-site Behavioral Targeting leverages each individual Web visitor's observed click-stream behavior, both on the current Web visit and from all previous visits, to decide what content is likely to be most effective to serve to that visitor."), *available at* http://www.omniture.com/offer/281) (last visited October 7, 2009).

[5] Felten, *supra* n.1, at 3-4; Chester, *supra* n.1, at 8-10; Electronic Frontier Foundation, How Online Tracking Companies Know Most of What You Do Online (and What Social Networks Are Doing to Help Them), Sept. 21, 2009, http://www.eff.org/deeplinks/2009/09/online-trackers-and-social-networks (last visited October 7, 2009).

[6] BALACHANDER KRISHNAMURTHY & CRAIG E. WILLS, ON THE LEAKAGE OF PERSONALLY IDENTIFIABLE INFORMATION VIA ONLINE SOCIAL NETWORKS (2009) *available at* http://conferences.sigcomm.org/sigcomm/2009/workshops/wosn/papers/p7.pdf (last visited October 6, 2009).

[7] *Id.*

then just go to your profile page, record its contents, and add them to their file."[8] Facebook recently settled a $9.5 million class action lawsuit involving its "Beacon" advertising program, which automatically creates posts on users' Facebook pages based on purchases or other actions on third-party websites.[9]

The collection of this online information is frequently being matched with real-world, offline identities. Professor Edward W. Felten testified before the committee about the process by which an online ad service might combine its user profile with information purchased from a commercial database: "If the ad service does know the identity, then third party services can provide a wealth of additional information, such as the user's demographics, family information, and credit history, which can be incorporated into the ad service's profile of the user, to improve ad targeting."[10] While Professor Felten was careful to make clear that "the fact that something is possible as a technical matter does not imply that reputable ad services actually do it,"[11] it seems likely the process is not uncommon. For example, the company Comscore, a leading provider of website analytic tools, boasts that "online behavioral data can…be combined with attitudinal research or linked with offline databases in order to diagnose cross-channel behavior and streamline the media planning process."[12]

The prevalence of online marketing is certainly growing—one online advertising CEO states that "[m]oving from site-targeting to people-targeting is the central dynamic of the industry"[13]—and consumers are increasingly concerned. A recent study from professors at the University of Pennsylvania and the University of California, Berkeley found that two-thirds of consumers objected to online tracking by advertisers, and that number rose on learning of the ways in which marketers are following their online behavior.[14]

II. Governmental access to these extensive personal profiles is possible and would be disastrous.

The issue before these subcommittees, then, is how to regulate the use of these profiles. It is no exaggeration to say these profiles—which may combine records of a person's entire online activity and extensive databases of real-word, personally identifiable information—draw a personal portrait unprecedented in scope and detail. Because the Internet has become intertwined with such personal facets our lives, the same

---

[8] EFF, *supra* n.5.
[9] *Internet Social Networking Sites Eye Privacy Expectations in Evolving Market*, BNA PRIVACY WATCH, Oct. 8, 2009 (discussing *Lane v. Facebook Inc.*, N.D. Cal., No. 08-3845).
[10] Felten, *supra* n.1 at 4.
[11] *Id.*
[12] Why Comscore?, http://comscore.com/About_comScore/Why_comScore (last visited October 6, 2009).
[13] Robert D. Hof, *Ad Networks Are Transforming Online Advertising*, BUSINESS WEEK, Feb. 19, 2009 (quoting Matt Spiegel of Omnicom Media) *available at* http://www.businessweek.com/magazine/content/09_09/b4121048726676.htm (last visited October 8, 2009).
[14] Stephanie Clifford, *Two-Thirds of Americans Object to Online Tracking*, N.Y. TIMES, Sept. 29, 2009 *available at* http://www.nytimes.com/2009/09/30/business/media/30adco.html (last visited October 8, 2009).

technology which has provided such tremendous advances also offers tremendous opportunities for government surveillance more intrusive than has ever before been possible. Imagine the government, without a warrant or any basis for individualized suspicion, reviewing records not just of what books a person had borrowed from a library, but also how she found the books, and what specific pages she read. We certainly wouldn't permit that in the offline world, and we shouldn't permit it online either.

We do not know if the government is already accessing these records, but we do know that the C.I.A., via its investment arm In-Q-Tel, has invested in a software company that specializes in monitoring blogs and social networks.[15] We also know the government has accessed, and likely continues to access, other private databases of personal information. For example, the Department of Defense, the C.I.A., and the F.B.I. have all purchased use of private databases from Choicepoint, one of the largest and most sophisticated aggregators of personal data.[16] In the words of the F.B.I., "We have the legal authority to collect certain types of information" because ChoicePoint is "a commercial database, and we purchase a lot of different commercial databases....They have collated information that we legitimately have the authority to obtain."[17]

The government has also sought access to some forms of online user data, for example the D.O.J. subpoenaed search records from Google, Yahoo!, and other search providers in order to defend a lawsuit.[18] In the words of Chris Hoofnagle, a senior fellow at the Berkeley Center for Law and Technology, "These very large databases of transactional information become honey pots for law enforcement or for litigants."[19] Given the government's demonstrated drive to access both online data and commercial databases of personal information, it seems nearly certain that law enforcement and other government actors will purchase or otherwise access the type of detailed profiles of online behavior compiled by behavioral marketers.

---

[15] Noah Shactman, *U.S. Spies Buy Stake in Firm That Monitors Blogs, Tweets*, WIRED, Oct. 19, 2009 *at* http://www.wired.com/dangerroom/2009/10/exclusive-us-spies-buy-stake-in-twitter-blog-monitoring-firm/ (last visited October 23, 2009).

[16] Shane Harris, *FBI, Pentagon Pay For Access to Trove of Public Records*, NAT'L J., Nov. 11, 2005, *available at* http://www.govexec.com/story_page.cfm?articleid=32802 (last visited October 7, 2009); Robert O'Harrow Jr., *In Age of Security, Firm Mines Wealth Of Personal Data*, WASHINGTON POST at A01, Jan. 20, 2005, *available at* http://www.washingtonpost.com/wp-dyn/articles/A22269-2005Jan19.html (last visited October 7, 2009).

[17] Harris, supra n.16 (quoting F.B.I. spokesman Ed Cogswell).

[18] Hiawatha Bray, *Google Subpoena Roils the Web, US Effort Raises Privacy Issues*, BOSTON GLOBE, January 21, 2006, *available at* http://www.boston.com/news/nation/articles/2006/01/21/google_subpoena_roils_the_web/ (last visited October 7, 2009).

[19] Miguel Helft, *Google Told to Turn Over User Data of YouTube*, NEW YORK TIMES, July 4, 2008 *available at* http://www.nytimes.com/2008/07/04/technology/04youtube.html (last visited October 6, 2009).

III. The existing law is inadequate.

Unfortunately, the existing law provides little protection:[20]

- Many legal analysts believe courts will find that the Fourth Amendment's guarantee against unreasonable search and seizures does not apply because of the "third party doctrine": the personal online data is "communicated" by a user to the web site owner, thus vitiating any reasonable expectation of privacy.[21]
- The Stored Communications Act, part of the Electronic Communications Privacy Act, is unlikely to provide substantial limitations on government access to the profiles created by behavioral marketers, because (1) the information may be in the possession of third-party entities not covered by the act,[22] and (2) if the Act applies, it is not clear what protection is accorded to clickstream data and the like, which may or may not constitute the "content" of a communication.[23]
- Although the Privacy Act of 1974[24] regulates systems of records that are created and maintained by the government, the Act does not apply to records obtained from a private party.[25]
- While a patchwork of other laws may provide some protection for certain kinds of records, like financial[26] and health[27] data or cable television[28] and video rental records,[29] these laws leave the vast majority of online data unprotected.

IV. Congress should pass new laws that restrict government access to this data, balancing effective law enforcement with the right to privacy.

A record of online behavior is at least as revealing as a record of a person's reading habits at a library. To safeguard autonomy, privacy, and intellectual freedom, our laws have long protected library records,[30] and to protect these same values, we need

---

[20] *See generally* John Palfrey, *The Public and the Private at the United States Border with Cyberspace*, 78 MISS. L.J. 241 (2008); Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083 (2002).

[21] *See* ORIN S. KERR, U.S. DEP'T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS § I.B.3 (Jan. 2001); Solove, *supra* n.20 at 1141.

[22] *See* 18 U.S.C. §§ 2702-03

[23] *See* 18 U.S.C. § 2520(8), §§2702-03.

[24] 5 U.S.C. § 552a.

[25] *See* Solove, *supra* n.20, at 1066.

[26] *See* Right to Financial Privacy Act, 12 U.S.C. §§ 3401-22.

[27] *See* Health Insurance Portability and Accountability Act of 1996 § 264, Pub. L. 104-191, 110 Stat. 1936, § 2033 (codified at 42 U.S.C. 1320d-2 note); 45 C.F.R. §§ 164.

[28] *See* Cable Communications Policy Act of 1984, 47 U.S.C. § 551.

[29] *See* Video Privacy Protection Act of 1988, 18 U.S.C. § 2710.

[30] 48 states protect library reading records by statute, *see, e.g.*, N.Y. C.P.L.R. § 4509; Cal. Gov. Code §§ 6267, 6254(j), and federal and state courts have also often frowned upon attempts by the government or civil litigants to gain access to such records, *see, e.g.*, *In re Grand Jury Subpoena to Amazon.com*, 246 F.R.D. 570, 573 (W.D. Wis. 2007) (quashing a government subpoena seeking the identities of 120 book buyers because "it is an unsettling and un-American scenario to envision federal agents nosing through the

similar protections for the privacy of our online behavior. Likewise, under existing law, the government must obtain a warrant supported by probable cause to gain access to stored electronic communications, even when those records are in the possession of a third party.[31] The digital profiles compiled by behavioral marketers are every bit as revealing as emails or other communications and so require the same level of protection. Therefore:

- To obtain access to personal profiles compiled by behavioral marketers, the government should be required to obtain a *warrant based on a showing of probable cause*, that a crime is being or has been committed.[32]
- Third party civil litigants seeking to subpoena such information should be required to provide notice to the subject of the information, and to show
  - a compelling interest in the information,[33]
  - that no less intrusive means exists,[34]
  - a prima facie validity of the action, and
  - that these factors outweigh the subject's First Amendment right to receive information anonymously.
- Persons aggrieved should have a private right of action.[35]

The Internet has been the engine of radical, positive changes in the way we communicate, learn, and transact commerce. And a number of the most important actors in this space are supported by advertising revenue. Still, as we appreciate what the Internet brings us, we must be wary. Behavioral marketers are creating digital portraits of unprecedented breadth and depth—portraits that will be irresistible to government investigators. Without the necessary legal restrictions on government access to these portraits, we will soon find the Internet has been transformed from a library and playground to a fishbowl, and that we have unwittingly ceded core values of privacy and autonomy.

---

reading lists of law-abiding citizens while hunting for evidence against somebody else."); *In re Grand Jury Subpoena to Kramerbooks & Afterwords, Inc.*, 26 Media L. Rep. (BNA) 1599, 1601 (D.D.C. 1998) (First Amendment requires government to "demonstrate a compelling interest in the information sought . . . [and] a sufficient connection between the information sought and the grand jury investigation" prior to obtaining book records); *Tattered Cover v. City of Thornton*, 44 P.3d 1044, 1059 (Colo., 2002) (government access to book records only passes muster under Colorado Constitution if "warrant plus" standard is met by the government—i.e, prior notice, adversarial hearing, and showing of a compelling need).

[31] *See* Electronic Communications Privacy Act, 18 U.S.C. § 2703(a).

[32] *See, e.g., Dumbra v. United States*, 268 U.S. 435, 439, 441 (1925); FED. R. CRIM. P. 41.

[33] See, e.g., *Kramerbooks*, 26 Media L. Rep. at 1601.

[34] *See, e.g., Tattered Cover*, 44 P.3d at 1059.

[35] *See* ECPA, 18 U.S.C. § 2707.

Thank you for your efforts to highlight this important privacy issue. If you have any questions, please contact Christopher Calabrese at 202-715-0839 or by email at ccalabrese@dcaclu.org.

Sincerely,

Michael W. Macleod-Ball
Acting Director, Washington Legislative Office

Christopher Calabrese
Legislative Counsel

BerkeleyLaw
UNIVERSITY OF CALIFORNIA

University of California, Berkeley
School of Law
396 Simon Hall
Berkeley, CA 94720-7200
1-510-643-0213
1-510-643-2362
http://bclt.berkeley.edu/
choofnagle@law.berkeley.edu

[Submitted via email to Earley Green, earley.green@mail.house.gov]

December 30, 2009

Representative John Dingell
2125 RHOB
Washington, DC 20515

Dear Representative Dingell,

Thank you for the opportunity to testify before the Subcommittee on Communications, Technology, and the Internet, and the Subcommittee on Commerce, Trade and Consumer Protection on November 19, 2009, at the joint hearing entitled, "Exploring the Offline and Online Collection and Use of Consumer Information." I have written answers to your questions below. Feel free to call upon me if I can be of any additional assistance.

Respectfully Submitted,

Chris Jay Hoofnagle

Questions from The Honorable John Dingell

1. By virtue of its use, is information collected about consumers rightly categorized as a commodity? Yes or no.

Yes. In *Reno v. Condon*, 528 U.S. 141 (2000), the Supreme Court held in an unanimous decision that personal information contained in the records of state motor vehicle departments, which was routinely sold in order to identify and target commercial solicitations, was an article of interstate commerce. Like personal information in motor vehicle databases, information collected about consumers in other contexts is bought and sold similar to other commodities. In fact, it is often sold in bulk, priced per thousand records.

2. Similarly, because the Federal government already regulates other types of commodities, should consumer information also be subject to Federal regulation? Yes or no?

Congress already regulates consumer information in several contexts, including video rental, cable viewing, financial services, and in credit granting. With that said, it is important to recognize the role of the states in protecting citizens' privacy. California, in particular, has been on the vanguard in the creation of innovative protections for personal data, including many of the rights to remedy and protect against identity theft that have been adopted at the federal level. A recent article by my colleague, Professor Paul Schwartz, describes several models that could preserve some ability of states to innovate in this field.[1] He suggests that preemption can be tailored to only apply to conduct required by the statute instead of the entire subject matter of the legislation. He also suggests "second-best" solutions, such as a plus-one approach (a federal standard that could be influenced by one state, which would still be empowered to legislate on the matter), and the simple approach of sun-setting preemption.

3. Moreover, if we consider consumer information a commodity, should the source from which it is derived (i.e., consumers) enjoy statutorily enumerated rights with regard to its collection and use? Yes or no.

To empower individuals, Congress should create rights with regard to the collection and use of information. Congress has already done so with respect to several types of personal information, including motor vehicle records, financial and credit information, and information about media consumption, such as video and cable records.

Privacy norms suggest that information should be collected directly from consumers. However, many marketing companies have found ways to collect information without directly involving the individual. (Most notably, through "enhancement.") Legislation should anticipate the continued practice of companies using indirect methods, and methods that obscure information collection from the consumer. Incentives should be created to collect data directly from the individual, because that gives the individual the opportunity to better understand and object to data collection and use.

[1] Paul M. Schwartz, *Preemption and Privacy* Yale Law Journal, 2009, available at SSRN: http://ssrn.com/abstract=1404082.

4. How would you characterize the general level of consumer awareness about his or her rights pertaining to the collection and use of his or her information for marketing purposes? Low, medium, or high?

Low. Research conducted at the University of California and University of Pennsylvania points to a consistent problem with consumer understanding of the rules and business practices surrounding personal information. These misunderstandings form one reason why market approaches have failed to address consumer privacy adequately. Consumers do not act to protect their privacy in the marketplace, because they believe it is already protected.

In my written testimony, I cited to several examples of this problem in Appendix I. I would like to call attention to an additional paper covering these issues in the online context by Aleecia McDonald and Professor Lorrie Cranor of Carnegie Mellon, titled, *An Empirical Study of How People Perceive Online Behavioral Advertising*, available at http://www.cylab.cmu.edu/research/techreports/2009/tr-cylab09015.html. This team found:

> ... We discovered that many participants have a poor understanding of how Internet advertising works, do not understand the use of first-party cookies, let alone third-party cookies, did not realize that behavioral advertising already takes place, believe that their actions online are completely anonymous unless they are logged into a website, and believe that there are legal protections that prohibit companies from sharing information they collect online. We found that participants have substantial confusion about the results of the actions they take within their browsers, do not understand the technology they work with now, and clear cookies as much out of a notion of hygiene as for privacy...

5. This in mind, do you believe more should be done to raise consumer awareness about the rights he or she enjoys with respect to the collection and use of his or her information? If so, who should do this?

Our research into consumer knowledge suggests that educational awareness campaigns will be of limited utility, and that they should not displace other types of interventions. Consumers believe that the law already protects personal information in a vigorous way. Thus, they are unlikely to spend time reading educational materials about rights they assume they already enjoy.

6. What statutorily enumerated rights do consumers currently possess to view the information collected about them, both online and offline?

In the online context, consumers do not have statutory rights to access or correct information about themselves.

In several offline contexts, consumers have enforceable statutory access and correction rights. Congress has created a wide array of statutes to govern the collection, use, and dissemination of personal information. They include:

- Fair Credit Reporting Act of 1970 (FCRA), Pub. L. No. 90-32, 15 U.S.C. §§1681 et seq.
    - The first federal information privacy law in the United States is highly complex, and includes elements of all eight OECD Privacy Guidelines, thus giving consumers a wide array of rights. The FCRA is a fascinating statute that strikes a bargain for information processing: highly-sensitive personal information can be collected and aggregated for credit, employment, and tenant screening purposes. To facilitate this, Congress eliminated individuals' defamation, invasion of privacy, and negligence suits for such data collection and use, absent malicious intent. This incredible power is balanced by a strong "maximum possible accuracy" standard integral to the statute, that should prevent the collection of irrelevant, unverifiable information, and creates an evolving standard for accuracy in covered databases. As with other federal privacy laws in the US, the FCRA is sectoral; it governs statutorily-defined "consumer reporting agencies," and limits "consumer reports" created by these agencies to certain employment, tenant screening, and credit uses. Consumers now have a right to obtain a free copy of their consumer report, to dispute inaccurate information, to prevent consumer reports for being used for secondary purposes, and to have derogatory information eventually be removed from the report.
- Cable Communications Policy Act of 1984 (CCPA), Pub. L. No. 98-549, 47 U.S.C. §551.
    - Regulates the collection, use, and dissemination of information by cable service providers. In some respects, the CCPA is the strongest US information privacy law. For instance, the law restrains even first party (the cable service provider's) collection of information about individuals' television viewing habits. The CCPA also requires that users be given access to data, and that user data be destroyed after it is no longer needed for service delivery. Cable service providers may sell their customer lists to third party marketers on an opt-out consent standard.
- Driver's Privacy Protection Act of 1994, Pub. L. No. 103-322, 18 U.S.C. §§2721–2725.
    - The DPPA restricts states from disclosing or selling personal information in state motor vehicle records. As with other major US privacy laws, the DPPA was enacted as a result of a controversy—attacks upon and the death of an individual who was located through motor vehicle records. As originally enacted, motor vehicle authorities could sell records to commercial entities on an opt out basis, but in 1998, an opt in standard was adopted. Since then, commercial entities have exploited other loopholes to obtain driver data.
- Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191 (Privacy Rule promulgated at 45 CFR § 460).
    - Resulted in promulgation of rules for the security and privacy of health information. Prior to HIPAA, medical privacy was regulated on a state-by-state basis. HIPAA created national standards that do not preempt state law (thus some state medical privacy

protections are more stringent). HIPAA allows transfer of medical information for treatment, payment, or health care operations purposes without patient consent. HIPAA's privacy rule creates requirements for privacy and security training, the appointment of an official responsible for privacy, a right to control appearing in a patient directory, and a right to control how medical information is communicated. Importantly, the rules created access rights to one's medical file, and the right to an auditing of disclosures. Now that auditing and access protections are in place, patients have discovered many cases where authorized users of records have abused their access, and have even sold personal information to news media entities.[2]

7. What statutes and/or regulations, whether Federal or state, exist to ensure that consumer information is not sold to those who would use it for nefarious purposes?

Firms have incentive conflicts when it comes to selling personal information. Although they wish to maintain a trusted relationship with consumers, they can gain revenue from quietly selling personal information to others, for legitimate or nefarious purposes. Perhaps the best check against selling data for nefarious purposes comes from access and audit log requirements in federal statutes such as the FCRA and the HIPAA Privacy Rule. These allow individuals to see who has gained access to their files. Especially in the HIPAA context, access and audit log requirements have exposed the problem of file "browsing," and even the sale of health information of celebrities to news agencies.

"Data provenance" is another approach that is underexamined in US law. "Data provenance" is the requirement that buyers and sellers of personal information exercise diligence to ensure against misuse of data. Several duties would be incorporated under provenance: a firm buying personal information would first investigate to determine that the data were fairly collected and that the sale does not contravene consumers' expectations. Sellers of data would screen buyers to ensure that data were not being sold to effectuate common frauds, such as sweepstakes promotions and the like. Data provenance responsibilities can create incentives to reduce gray and black market sales of personal information, and some information firms already perform these duties.

8. Do you believe industry is doing an adequate job of protecting the security of consumer information it collects, including ensuring it not be sold to irresponsible parties? If not, what should be done to remedy this?

The hearing witnesses represented mainstream companies with best-in-industry practices. Nevertheless, other firms in the marketplace seem to be deluging consumers with clearly fraudulent advertising, for everything from sweepstakes to weight loss products. A search on nextmark.com's list finder for

[2] Former UCLA hospital worker admits selling celeb medical records, USA Today, Dec. 1, 2008, available at http://www.usatoday.com/life/people/2008-12-01-UCLA-records_N.htm.

"impulsive" produces 241 databases of consumer information. "Mature" nets 536. The sellers of these databases deserve more scrutiny.

The problem in the information privacy field is similar to many other areas of self-regulation. Some actors are responsible stewards of personal information, some are not. Without enforceable rights, consumers can neither learn of information privacy problems nor police them. Thus, consumers are reliant upon state attorneys generals and the Federal Trade Commission to detect distributed frauds, investigate, and remedy them. Data provenance responsibilities and audit log requirements could give consumers tools to self-police this trade.

9. In her testimony, Ms. Bougie asserts that privacy legislation will place small businesses at a disadvantage vis-à-vis larger companies. Do you believe this is true? If not, why?

One way to place smaller firms on the same field as larger ones would be to address affiliate sharing of data. US information privacy law generally allows affiliates to share information to an unlimited degree, thus giving larger firms an advantage over smaller ones.

With the explosive growth in the size of firms, and the completely unrelated business lines of these conglomerates, such affiliate sharing likely contravenes consumers' expectations. The KnowPrivacy Report clearly illustrates this issue.[3] Researchers of that report wrote to popular websites requesting a disclosure of their affiliate structure, but received few replies, most of which were not responsive. They found:

> "In our analysis of the privacy policies we found that 46 of the top 50 companies affirmatively state that they share data with affiliates, and the four remaining were unclear. We sent each company a request via email or an online web form for a list of each affiliate they may share data with. We received 14 replies, but none included the lists we asked for…
>
> […]
>
> "MySpace, one of the most popular social networking sites (especially among younger users), is owned by NewsCorp, which has over 1500 subsidiaries…Information pulled from these websites could potentially find its way to all of these affiliated companies.

[3] Joshua Gomez, Travis Pinnick, and Ashkan Soltani, KnowPrivacy, available at http://knowprivacy.org/affiliates.html.

10. Industry claims to practice self-regulation in the collection and use of consumer information. This being the case, what would be the harm to industry in mandating under statute similar such regulation?

Overly broad legislation could create reification and a compliance mindset among data companies. Legislation should encourage an evolving standard of best practices that give firms incentives to expand consumers' rights in data. One notable example of this is the FCRA's "maximum possible accuracy" standard. Congress recognized in 1970 that credit reporting database technology would evolve, and thus placed consumer reporting agencies under a duty to continually improve their systems. Data privacy legislation in this field should take a similar approach that gives incentives for improving practices with time.

Congress of the United States

House of Representatives

COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6115

MAJORITY (202) 225-2927
FACSIMILE (202) 225-2525
MINORITY (202) 225-3641

energycommerce.house.gov

December 16, 2009

Mr. George V. Pappachen
Chief Privacy Officer
Kantar/WPP
11 Madison Avenue, 12th floor
New York, New York 10010

Dear Mr. Pappachen:

Thank you for appearing before the Subcommittee on Communications, Technology, and the Internet, and the Subcommittee on Commerce, Trade, and Consumer Protection on November 19, 2009, at the joint hearing entitled "Exploring the Offline and Online Collection and Use of Consumer Information".

Pursuant to the Committee's Rules, attached are written questions for the record directed to you from certain Members of the Committee. In preparing your answers, please address your response to the Member who submitted the questions and include the text of the question with your response, using separate pages for responses to each Member.

Please provide your responses by January 8, 2010, to Earley Green, Chief Clerk, in Room 2125 of the Rayburn House Office Building and via e-mail to Earley.Green@mail.house.gov. Please contact Earley Green or Jennifer Berenholz at (202) 225-2927 if you have any questions.

Sincerely,

Henry A. Waxman
Chairman

Attachment

To: The Honorable John Dingell

Please find below my responses to the written questions stemming from my appearance before the Subcommittee on Communications, Technology, and the Internet, and the Subcommittee on Commerce, Trade, and Consumer Protection on November 19, 2009, at the joint hearing entitled "Exploring the Offline and Online Collection and Use of Personal Information".

1. By virtue of its use, is information collected about consumers rightly categorized as a commodity?

No. While there may be some class of consumer data that may be suited for such handling at some point, I certainly do not think the marketplace is near agreed on core issues such as value, ownership and other attributes that are typically characteristic of a commodity.

2. Similarly, because the Federal government already regulates other types of commodities, should consumer information also be subject to Federal regulation?

No. This is in keeping with my assertion that I do not think that consumer information as broadly referenced is in position to receive commodity classification.

3. Moreover, if we consider consumer information a commodity, should the source from which it is derived (*i.e.*, consumers) enjoy statutorily enumerated rights with regard to its collection and use?

No. This response is again in keeping with my assertion that I do not think that consumer information as broadly referenced is in position to receive commodity classification. I would also restate that while there may be some class of consumer data that may be suited for statutory treatment at some point, I do not think the marketplace has reached agreement on defining issues that typically underpin such an endeavor.

4. How would you characterize the general level of consumer awareness about his or her rights pertaining to the collection and use of his or her information for marketing purposes?

Low. Research suggests that consumers are not generally aware of their rights around collection and use. In some respect, consumers evince an implicit reliance (whether justified or not) on a secure system whose details are not overly familiar to them and which they have not investigated in large numbers.

5. This in mind, do you believe more should be done to raise consumer awareness about the rights he or she enjoys with respect to the collection and use of his or her information? If so, who should do this?

Yes, I believe that various stakeholders have a role to play in increasing awareness. For example, the online industry's introduction of a self-regulatory framework which introduced consumer education as a core tenet establishes the role industry must play in this area. The most effective initiatives will be a collaboration of governmental and industry bodies.

6. Do you believe industry is doing an adequate job of protecting the security of consumer information it collects, including ensuring it not be sold to irresponsible parties? If not, what should be done to remedy this?

I think the majority of marketplace actors are responsible in their treatment of consumer information, particularly personal information. Most trade associations require members to securely protect consumer and customer personal information in their possession. However, there may be actors that fall outside this paradigm. To address this outlier concern, I believe a combination of legislative and regulatory initiative is appropriate to protect the security of consumer information in the possession of commercial and other actors.

7. In her testimony, Ms. Bougie asserts that privacy legislation will place small businesses at a disadvantage vis-à-vis larger companies. Do you believe this is true? If not, why?

I think compliance in general is more imposing on small businesses than others. The marketing industry, which includes small businesses, have invested in certain privacy regimes (for ex. notice and consent for online information) that are established components of their business routine. In many cases, the business infrastructure that has evolved can be substantially disrupted by legislation – depending very much on the details of the legislative approach, of course. For example, an opt-in requirement for the collection of basic information at smaller websites could deal a death blow. Even a requirement to re-work privacy policies suggests a different coordination for small businesses which inevitably translates to additional legal and operational costs and the use of resources that are typically not resident within their more limited organizations.

8. Industry claims to practice self-regulation in the collection and use of consumer information. This being the case, what would be the harm to industry in mandating under statute similar such regulation?

The harm would be very dependant on the legislative approach and how truly similar statutory treatment is to self-regulatory efforts. Some aspects of the self-regulatory model recognize concepts whose implementation allows industry actors to evolve their methods to align with market developments. For example, development of consumer messaging for the purposes of privacy protection that is produced from the perspective of brand communications has the advantage of leveraging industry knowledge and experience in this area. This allows for a flexible approach and an evolution that is in keeping with actual market movements. I believe legislation can lead to a different orientation, an intention to strictly tailor to the minimum requirements posted in the rules.

It removes the obligation on the part of industry to evolve the protection framework in lock step with the leading industry practices. This said, a complementary legislative approach that is fashioned to recognize self-regulatory schemes and yet corrals rogue actors can be effective.

Congress of the United States

House of Representatives

COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6115

MAJORITY (202) 225-2927
FACSIMILE (202) 225-2525
MINORITY (202) 225-3641

energycommerce.house.gov

December 16, 2009

Ms. Jennifer T. Barrett
Global Privacy and Public Policy Executive
Acxiom
601 East 3rd Street
Little Rock, AR 72201

Dear Ms. Barrett:

Thank you for appearing before the Subcommittee on Communications, Technology, and the Internet, and the Subcommittee on Commerce, Trade, and Consumer Protection on November 19, 2009, at the joint hearing entitled "Exploring the Offline and Online Collection and Use of Consumer Information".

Pursuant to the Committee's Rules, attached are written questions for the record directed to you from certain Members of the Committee. In preparing your answers, please address your response to the Member who submitted the questions and include the text of the question with your response, using separate pages for responses to each Member.

Please provide your responses by January 8, 2010, to Earley Green, Chief Clerk, in Room 2125 of the Rayburn House Office Building and via e-mail to Earley.Green@mail.house.gov. Please contact Earley Green or Jennifer Berenholz at (202) 225-2927 if you have any questions.

Sincerely,

Henry A. Waxman
Chairman

Attachment

Answers for the Honorable John Dingell

1. By virtue of its use, is information collected about consumers rightly categorized as a commodity?

   Answer: No. We understand a "commodity" to be an economic good or service demanded without qualitative differentiation. That is, the market considers it to be the same regardless of who produces or sells it, an effect of which is that its price is determined across the entire market.

   While data can, and does, provide economic good, it is usually not mass-produced or unspecialized. Instead, information is frequently created and assembled "on-demand," Part of what gives information its value is its uniqueness; there is usually little demand for it without qualitative differentiation. Specific information collected about consumers has value, is traded and sold or bartered, sometimes by the individual themselves, but is done in a specific way with the intent of being used for a specific purpose.

2. Similarly, because the Federal government already regulates other types of commodities, should consumer information also be subject to Federal regulation?

   Answer: Information uses are susceptible to federal regulation, with important qualifications, though not because the federal government already regulates commodities.

   Even though information is not a commodity, some uses, and some types of information are already regulated and others should be regulated in the future. Commercial uses which can result in harm to consumers can - and in specific instances should - be regulated. For example, data collection is already regulated when used for determining credit and employment by the FCRA. Use of medical information from health care providers is regulated by HIPAA. These types of high risk uses and certain sensitive information should continue to be regulated and these regulations possibly refined over time as new sources of information evolve. Certain uses of information which can result in discrimination or embarrassment of individuals should be considered for regulation. Criminal convictions that bear no rational relationship to the applicant's prospective job role, should be closely scrutinized. However, not all uses of information need regulation. The sale of lists for marketing purposes is not regulated by law, but is covered by industry codes of conduct. For over 30 years, this has been an adequate form of regulation and should be encouraged to continue as marketing information collection and use evolves. Because self-regulatory codes can evolve more easily than law, if Government were to endorse industry codes of conduct as a "safe harbor" against unfair and deceptive trade practices, it would encourage companies who are not members of those organizations to follow the codes of conduct that have proven to work. This is often referred to a co-regulation or regulated self-regulation. An article on this concept can be found at http://www.osce.org/publications/rfm/2004/12/12239_93_en.pdf.

3. Moreover, if we consider consumer information a commodity, should the source from which it is derived, (i.e. consumers) enjoy statutorily enumerated rights with regard to its collection and use?

   Answer: No. See answer to question #2.

   Irrespective of any question of information being a commodity, individuals' expectations regarding information about them evolve. Over a century ago, some considered the publication of photographs in newspapers, then newly possible as a result of technological advance, to raise serious privacy concerns for citizens in a busy street going about their daily lives. Such publication is a "use" of information about consumers

(i.e., their likenesses). Few would argue that individual rights in such an instance would need to be statutorily enumerated.

4. How would you characterize the general level of consumer awareness about his or her rights pertaining to the collection and use of his or her information for marketing purposes?

   Answer: Awareness varies with the type of collection. Most consumers have understood for years that if they buy from a catalog, they will receive catalogs from other companies and they can opt-out from this practice. Awareness about this type of collection is relatively high. However, many consumers are unaware that, analogous to the catalog example, on the web cookies are used to determine their preferences and deliver personalized content and marketing messages and that here too they can opt-out of or block this practice. Recent attention to this practice has increased awareness, but if consumers took better advantage of available information that describes these practices, we believe it would reduce mistrust.

5. This in mind, do you believe more should be done to raise consumer awareness about the rights he or she enjoys with respect to the collection and use of his or her information? If so, who should do this?

   Answer: Yes.

   We need a more informed consumer. It is the joint responsibility of industry and government, as well as consumers themselves, to educate consumers. A model of what government should do is found in the awareness and education campaign the FTC has conducted in recent years about ID theft. Innovative ways to inform the consumer also should be encouraged from industry like the privacy setting in all new browsers. A joint effort between industry and government will provide the best results.

6. Do you believe industry is doing an adequate job of protecting the security of consumer information it collects, including ensuring it not be sold to irresponsible parties? If not, what should be done to remedy this?

   Answer: With respect to Acxiom and sophisticated businesses generally, yes.

   We believe that the security provided to consumer information, while not perfect, is for the most part adequate. These protections have been enhanced by notifications about breaches required by laws in most states. A single federal standard in this area would make compliance easier, but would not substantially change protections.

   We also believe most companies understand their responsibility when they sell information about their customers for legitimate purposes, such as marketing or fraud prevention, by screening the purchaser to assure they have a legitimate business and need for the information. However, there will always be companies who misuse information in ways that could result in harm to consumers. We believe that enforcement by the FTC against unfair and deceptive trade practices under its existing authority can address the bad actors.

7. In her testimony, Ms Bougie asserts that privacy legislation will place small business at a disadvantage vis-à-vis larger companies. Do you believe this is true? If not, why?

   Answer: It could be.

   If legislation is not very carefully crafted, it will place significant burdens on small businesses in the form of compliance obligations and make access to information for

marketing and risk purposes harder and more expensive resulting in diminishing the ability of small business to market and grow their market. Large companies may be better able to absorb (or already have absorbed) compliance costs, such as for maintaining information security, than smaller companies.

8. Industry claims to practice self-regulation in the collection and use of consumer information. This being the case, what would be the harm to industry in mandating under statute similar such regulation?

Answer: Laying aside the potential First Amendment issues attendant with government regulation of speech, some assume there would be little harm if the government regulation is the same as the self-imposed regulation. As mentioned in the answer to question #2, if government endorsed industry codes of conduct as a "safe harbor" against unfair and deceptive trade practices, it would encourage companies who are not members of those organizations to follow the codes of conduct that have proven to work and allow for more flexibility to deal with evolving technologies and business practices. Such a legislative device is not uncommon and has been deployed in other arenas by the Committee on Energy & Commerce under your Chairmanship. Again, we believe it is appropriate in this context.

December 16, 2009

Ms. Zoe Strickland
Vice President, Chief Privacy Officer
Wal-Mart Stores Inc.
Wal-Mart Privacy Office
508 SW 8th Street, Mail Stop 0505
Bentonville, AR 72716

Dear Ms. Strickland:

Thank you for appearing before the Subcommittee on Communications, Technology, and the Internet, and the Subcommittee on Commerce, Trade, and Consumer Protection on November 19, 2009, at the joint hearing entitled "Exploring the Offline and Online Collection and Use of Consumer Information".

Pursuant to the Committee's Rules, attached are written questions for the record directed to you from certain Members of the Committee. In preparing your answers, please address your response to the Member who submitted the questions and include the text of the question with your response, using separate pages for responses to each Member.

Please provide your responses by January 8, 2010, to Earley Green, Chief Clerk, in Room 2125 of the Rayburn House Office Building and via e-mail to Earley.Green@mail.house.gov. Please contact Earley Green or Jennifer Berenholz at (202) 225-2927 if you have any questions.

Sincerely,

Henry A. Waxman
Chairman

Attachment

Walmart
Save money. Live better.

702 SW 8th Street
Bentonville, AR 72716

January 13, 2009

The Honorable John Dingell

1. By virtue of its use, is information collected about consumers rightly categorized as a commodity? Yes or no.

   Answer: No. Unlike pencils or widgets, customer information relates to real people. The impact to them must be considered as information is collected, used, and shared. We recognize that, although businesses may get value from the information, consumer impacts are of the utmost importance.

2. Similarly, because the Federal government already regulates other types of commodities, should consumer information also be subject to Federal regulation? Yes or no?

   Answer: To the extent privacy is regulated, it should be regulated as part of consumer protection, rather than as a commodity. Few areas more clearly involve interstate commerce, so federal rules are most appropriate if this area is regulated.

3. Moreover, if we consider consumer information a commodity, should the source from which it is derived (*i.e.*, consumers) enjoy statutorily enumerated rights with regard to its collection and use? Yes or no.

   Answer: In accordance with our responses above, we do not consider consumer information a commodity. However, many statutory or regulatory schemes exist to protect consumers. The use of consumer information falls under that umbrella. Besides protecting consumers, such rules could benefit industry as well. They could provide basic principles and rules of the road that could be applied in many contexts and technologies. These principles do not exist today, which could advantage companies with poor practices. We provide what we consider the benefits and risks to legislation or regulation in our responses below.

Walmart

4. How would you characterize the general level of consumer awareness about his or her rights pertaining to the collection and use of his or her information for marketing purposes? Low, medium, or high?

   Answer: Medium. I believe consumers know more about this area than some companies or policy-makers attribute to them. As an example, consumers understand how to prevent marketing messages – hence the large rate of sign-ups for the federal do-not-call list – or conversely how to sign up for applications on their mobile devices. Our office also receives 15-20 communications weekly from consumers regarding privacy, which can show a broader understanding of privacy issues. (In our privacy policy, we have provided a variety of channels – email, mail, and phone – for consumers to contact us about any privacy questions or concerns they may have.) On the other hand, consumers may have less understanding about back-end practices that may impact them, like how data may be acquired or shared more broadly than the companies they believe they are interacting with.

   We believe that statutory or regulatory protections should focus on practices that have impact on consumers. In our experience, consumers are interested in practices that impact them, not abstract concepts of data management or uses that facilitate the relationship (like internal and external data sharing to fulfill transactions). To be effective, protections need to be principles-based and able to be clearly communicated. As an example, what are the principles or triggers when consumer notice and/or choice should be offered? We believe a principles-based approach will drive the most meaningful impact and value for consumers.

5. This in mind, do you believe more should be done to raise consumer awareness about the rights he or she enjoys with respect to the collection and use of his or her information? If so, who should do this?

   Answer: Yes. Consumers could be provided with more information and options about data practices. Companies can do this, as can policy-makers through education or rule-making. To be most effective, messages and choices should be simple and clear, and adaptable over many technologies or interactions. This is not because the issues are too complicated for consumers to understand. Rather, based on our extensive experience with consumers, regarding privacy or otherwise, they are often stretched for time and have many diverse daily items to manage. Icons and clear choices are helpful. As part of clear choices, consistency of language could help consumers understand their options. For instance, if companies are offering the same choice (eg related to data sharing), consistent wording of that choice can minimize confusion, legalese, or loopholes. Harmful practices should simply be restricted or prohibited.

6. Do you believe industry is doing an adequate job of protecting the security of consumer information it collects, including ensuring it not be sold to irresponsible parties? If not, what should be done to remedy this?

   Answer: Yes. We believe companies have increased security measures considerably. This is borne out by numerous industry studies. That being said, security can always be improved. The sale or transfer of data is only a security issue if the transfer is unauthorized, for instance if a system is breached. Except for those instances, the sale or transfer of data is a business practice or policy. This is why privacy is a broader focus than security. Practices deemed harmful should be restricted or prohibited. For other practices, consumers should have clear notice and simple choices. As a point of reference, Walmart does not sell customer data, and only shares data with third parties for their own purposes if consumers have expressly consented (opted-in) to that data sharing.

7. In her testimony, Ms. Bougie asserts that privacy legislation will place small businesses at a disadvantage vis-à-vis larger companies. Do you believe this is true? If not, why?

   Answer: Not necessarily. There are a couple of reasons why smaller businesses may not be disadvantaged by privacy legislation. Given both their resources and access to data, large companies can do significantly more with data, and with a level of technological sophistication, that is likely unavailable to a small business. Moreover, many small businesses may not rely on the use or manipulation of customer data to a great extent. For example, they may rely more on traditional media like radio and newspaper ads, coupons, and gift cards. It is possible that clear federal standards could guide companies of all sizes, if they establish basic principles and do not present a complicated compliance burden.

8. Industry claims to practice self-regulation in the collection and use of consumer information. This being the case, what would be the harm to industry in mandating under statute similar such regulation?

   Answer: The point is well-taken that legislation based on responsible practices that are already part of self-regulation could help industry in some respects. Legislation could serve to screen out bad actors, and also provide principles for good data practices. Industry benefits from stability and certainty, particularly in ways that serve customers.

In this debate, I believe industry is concerned about two things. One concern is legislation that extends beyond establishing these basic rules, particularly in ways that negatively interfere with customer relationships; that create an unnecessarily complex compliance burden; or that are unworkable across different channels and technology. As an example that we typically raise, legislative solutions that are based on online practices – and that really only work in an online environment – should not simply be transferred to offline practices or interactions. Pop-up notices with hyperlinks would be an example. Instead, legislative solutions should be based on principles that reflect consumer protection, and that can be applied across channels and technology. We believe this approach is better for business and consumers. Such an approach is clearer and easier to communicate, and will also be more likely to achieve desired legislative goals.

A second concern involves liability risk. This is a concern regardless of whether the terms of the legislation reflect solid industry practice or self-regulation. A major concern would be any standard that looked like strict liability. This would be a significant cost to businesses and consumers, as a great many businesses manage consumer data. Instead, liability should be based on actual impacts to consumers, and should be enforced by federal or state regulators rather than private actions. This is very similar to the risk of harm standard that is embedded in federal bills and most state laws that relate to sending consumers notices of potential data breaches.

December 16, 2009

Ms. Michelle Bougie
Senior Internet Marketing Manager
LearningResources.com &
EducationalInsights.com
380 N. Fairway Drive
Vernon Hills, IL 60061

Dear Ms. Bougie:

Thank you for appearing before the Subcommittee on Communications, Technology, and the Internet, and the Subcommittee on Commerce, Trade, and Consumer Protection on November 19, 2009, at the joint hearing entitled "Exploring the Offline and Online Collection and Use of Consumer Information".

Pursuant to the Committee's Rules, attached are written questions for the record directed to you from certain Members of the Committee. In preparing your answers, please address your response to the Member who submitted the questions and include the text of the question with your response, using separate pages for responses to each Member.

Please provide your responses by January 8, 2010, to Earley Green, Chief Clerk, in Room 2125 of the Rayburn House Office Building and via e-mail to Earley.Green@mail.house.gov. Please contact Earley Green or Jennifer Berenholz at (202) 225-2927 if you have any questions.

Sincerely,

Henry A. Waxman
Chairman

Attachment

The Honorable John Dingell

1. *By virtue of its use, is information collected about consumers rightly categorized as a commodity? Yes or no.*

Answer: No. The definition of "commodity" on dictionary.com is "A generic, largely unprocessed, good that can be processed and resold. Commodities traded in the financial markets for immediate or future delivery are grains, metals, and minerals. They are generally traded in very large quantities." Although direct marketing consumer information is acquired (for use) in bulk, the economic value of consumer information depends on source, purchasing history and other circumstances. Consumer information is not fungible (two names-and-addresses are not of equal value) and direct marketers are not indifferent to the source or characteristics of the consumer information.

2. *Similarly, because the Federal government already regulates other types of commodities, should consumer information also be subject to Federal regulation? Yes or no?*

Answer: No. Information should not be subject to regulation without demonstrated need as a one-size-fits-all policy would not work for businesses in different industries and/or channels or of different sizes. This risk would be greatest for small businesses who must rent consumer information to expand their markets – not all companies generate sufficient leads to avoid prospecting with rented consumer names-and-addresses. I believe it is inappropriate to equate corn futures and consumer information for regulatory purposes.

3. *Moreover, if we consider consumer information a commodity, should the source from which it is derived (i.e., consumers) enjoy statutorily enumerated rights with regard to its collection and use? Yes or no.*

Answer: No. In this case, market forces provide effective protection against abuse of consumer information. Good marketing practices, widely adopted because of the leadership of industry groups and leading merchants, make unethical behavior much more difficult and infrequent. The direct marketing industry has a strong economic incentive to follow best practices because the consumer rules the markets; if consumers don't like a business practice or feel that trust has been violated, their revenge in the marketplace is enough to put most businesses away (especially in the online marketplace). I do not believe that Federal regulation will improve these results. New risks of liability created by unnecessary regulation will eventually result in lower economic activity without any compensating benefit.

4. *How would you characterize the general level of consumer awareness about his or her rights pertaining to the collection and use of his or her information for marketing purposes? Low, medium, or high?*

Answer: We believe that the right answer is "medium", largely because of media publicity and the considerable efforts of online merchants to be transparent about their data collection processes. It is worth noting that the use of consumer information in the direct mail business is decades old. Who hasn't received catalogs from unknown companies unsolicited in the mail? We believe consumers are well-aware of the existence of mailing lists and their prevalent use in our economy. It is our experience that consumers know how to remove themselves from both mailing lists and email lists, and frequently avail themselves of their right to "opt out".

5. *This in mind, do you believe more should be done to raise consumer awareness about the rights he or she enjoys with respect to the collection and use of his or her information? If so, who should do this?*

Answer: We believe that the issue of use and abuse of consumer information is an issue of trust that confronts the direct marketing industry. The industry has strong incentives to invest in earning and retaining the trust of consumers, in part through good communication practices about privacy policies. The industry has acted preemptively to build strong compliance with standards for privacy and data collection. By relying on industry self-policing, the market will perform efficiently and the cost of regulation will be kept to a minimum.

6. *Do you believe industry is doing an adequate job of protecting the security of consumer information it collects, including ensuring it not be sold to irresponsible parties? If not, what should be done to remedy this?*

Answer: Based on our experience and knowledge of the market, we believe the direct marketing industry does a good job protecting consumer information. In our experience, it is not possible to "buy" consumer information. The "sale" of consumer information is a common myth. Since companies expend a great deal of effort and resources to gather and accumulate valuable consumer information, they will not sell it, preferring instead to "rent" it so that its value can be exploited again and again. Thus when we use someone else's consumer information, we must pay a fee for a "one time" use. We do not have access to the information directly, only the right to use it. As a consequence, it is likely that we have rented and re-rented the same name-and-address many times over the years – each time we rent names, we have no way of knowing which names we are renting. In fact, a significant challenge facing direct merchants is validating the quality and effectiveness of mailing lists. Direct merchants attempt to match purchase information back to the origin of the names using coding and other means to determine if a list "performs" well. If the list generated sufficient revenue, one might choose to rent it again. Otherwise, the list will not get repeat business.

For these reasons, we believe that economic incentives drive the industry to do a thorough job of protecting consumer information. It is very much in the industry's financial interest to protect consumer information from leaking out. If the information becomes available to renters, future revenue would be cut off.

7. *Industry claims to practice self-regulation in the collection and use of consumer information. This being the case, what would be the harm to industry in mandating under statute similar such regulation?*

Answer: Adding new regulation is a slippery slope, especially if it is unnecessary. Regulation creates a target for enterprising plaintiff lawyers, which could hobble the industry. Furthermore, new regulation invites further regulation. It is unclear where regulation would end as it is always tempting to add to regulations already on the books. As noted above, the industry enjoys both a direct and indirect economic incentives to enforce good practices. Additional regulation is likely to distort the equilibrium that is working well in the marketplace, resulting in less commerce and a weaker American economy. We must never forget that the Internet is one of America's great job creators today.

New privacy regulations may have the unintended consequence of limiting future economic expansion by interfering in how businesses interact with consumers in the "digitized" economy. As emerging technologies continue to go mainstream, the way companies go to market, conduct commerce and interact will move well beyond reaching consumers in their "physical" mailbox. Regulations will slow the pace of these developments and ultimately restrict the ability of businesses to grow. We are particularly concerned that the impact of such regulation would be felt most profoundly by small businesses. Industry self-regulation of the collection and use of consumer data allows for the continued creativity, technology evolution and job expansion demanded by the American public.

2033 San Elijo Avenue, #402
Cardiff by the Sea, CA 92007

January 8, 2010

The Honorable John D. Dingell
Chairman Emeritus, Committee on Energy and Commerce
U.S. House of Representatives
Washington, DC 20515

Dear Chairman Emeritus Dingell:

Thank you for your follow-up questions pursuant to the November 19, 2009 hearing regarding "Exploring the Offline and Online collection and User of Consumer Information " before the Subcommittee on Communications, Technology, and the Internet and the Subcommittee on Commerce, Trade, and Consumer Protection.

Attached please find my responses to your questions. If there is any additional information or research that I might provide to you, please do not hesitate to contact me.

Thank you for your interest in these important consumer issues.

Sincerely,

Pam Dixon
Executive Director,
World Privacy Forum

Attachment

Responses of Pam Dixon, World Privacy Forum, to the Honorable John Dingell

1. By virtue of its use, is information collected about consumers rightly categorized as a commodity? Yes or no.

Yes. Information collected about consumers is a commodity.

2. Similarly, because the Federal government already regulates other types of commodities, should consumer information also be subject to Federal regulation? Yes or no?

Yes. The government already regulates certain consumer information, for example, consumer's financial information held by credit bureaus is regulated via the Fair Credit Reporting Act and FACTA.

3. Moreover, if we consider consumer information a commodity, should the source from which it is derived (*i.e.*, consumers) enjoy statutorily enumerated rights with regard to its collection and use? Yes or no.

Yes.

4. How would you characterize the general level of consumer awareness about his or her rights pertaining to the collection and use of his or her information for marketing purposes? Low, medium, or high?

Extremely low. Consumers are almost completely unaware of their rights regarding information collection and marketing use of the same.

5. This in mind, do you believe more should be done to raise consumer awareness about the rights he or she enjoys with respect to the collection and use of his or her information? If so, who should do this?

Yes, more should be done to raise consumer awareness of their rights. For example, consumers have the right to find out about their information held by specialty credit bureaus under the FCRA and FACTA. The MIB Group is an example of one such specialty credit bureau. (See http://www.mib.com/html/mib_privacy_policy.html) Another example is Scan Check (See http://www.nobouncedchecks.com/SCAN-check.html).

No comprehensive list of specialty credit bureaus exists for the public. Industry does not maintain a public list, nor does the Federal Trade Commission. So while consumers have the *right* to see their specialty credit bureau reports, in practical terms, it would be quite challenging for consumers to fully *exercise* this right because consumers do not know about these bureaus and would have difficulty finding even a handful of them on their own.

Additionally, the quality of privacy notices on the specialty bureau web sites regarding consumers' right to acquire a specialty report is of widely variable quality. Consumers who do manage to find a specialty credit bureau relevant to their information may not always have sufficient information from the company itself to exercise their rights under the FCRA/FACTA. This is just one small area of consumer information, many others exist and would benefit from additional consumer education.

The Federal Trade Commission is likely the correct place for a consumer education effort in this area, given the Commission's good track record on consumer education on other issues such as identity theft.

6. What statutes and/or regulations, whether Federal or state, exist to ensure that consumer information is not sold to those who would use it for nefarious purposes?

Regrettably, no significant statutes or regulations meaningfully touch the issue of ensuring consumer information is not sold to those who would use it for nefarious purposes. While some sectoral regulations such as HIPAA and some of the HI TECH Act do prohibit sales or marketing of some medical information held by certain entities, and while additional sectoral regulations, such as GLB and FACTA do carve out some narrow protections and rights for consumers in some areas, these statutes and regulations do not address the problems of broad secondary use of consumer information, particularly when that information is held by commercial databrokers.

7. Do you believe industry is doing an adequate job of protecting the security of consumer information it collects, including ensuring it not be sold to irresponsible parties? If not, what should be done to remedy this?

Industry is not doing an adequate job of protecting the security of the consumer information it collects, and it is not adequately ensuring that the information is not sold to irresponsible parties. The high levels of consumer harm in the current marketplace suggest that commercial data brokers, as an unregulated industry, need statutory controls to ensure consistent good behavior and best practices.

Having said that, it must be acknowledged that the issue of how to approach regulating the use of consumer information is a complex one; in seeking statutory remedies I believe the FCRA and FACTA are likely the best models to draw from. The FCRA approach of giving consumers certain informational rights and giving industry certain responsibilities regarding information handling has proven overall to be an effective approach over the years.

Certainly, the right to see what information is held by a company, where that information has been sold, the right to correct the information, and ideally, the right to delete information that could be characterized as inappropriately casting a consumer in a pejorative light would be important rights to grant to consumers. (For example, information that characterizes an elderly man or woman as an "impulse buyer," or an

individual listed with a mental illness characterized as "extremely receptive" to certain marketing campaigns, and so forth.)

8. In her testimony, Ms. Bougie asserts that privacy legislation will place small businesses at a disadvantage vis-à-vis larger companies. Do you believe this is true? If not, why?

Privacy legislation would not place small businesses at a disadvantage vis-à-vis larger companies. Much of the purpose of privacy legislation in the consumer information area should be to curtail egregious practices of bad actors. Ms. Bougie's business should be able to purchase and use marketing lists in an appropriate manner. Appropriately crafted privacy legislation would not hamper legitimate small business activities such as this, nor should it create onerous extra costs that would come to rest in particular on a small business.

What appropriately crafted legislation would ideally reign in would be the activities that bring harm to consumers, such as selling mental health information, medical information, sensitive financial information, and compiling databases to create marketing profiles of consumers that can lead to various forms of redlining. If small businesses are using appropriate consumer information in appropriate ways, then they should not be deleteriously impacted by consumer privacy legislation.

9. Industry claims to practice self-regulation in the collection and use of consumer information. This being the case, what would be the harm to industry in mandating under statute similar such regulation?

Industry has repeatedly stated that the DMA guidelines are a principled set of guidelines that protect consumers and constitute a fair self-regulatory approach that they (industry) are employing to great effect. (See *Guidelines for Ethical Business Practice*, Direct Marketing Association, http://www.dmaresponsibility.org/Guidelines/) If that is the case, I do not see a reason why current best practices and self-regulatory efforts such as the DMA Guidelines would harm industry if those practices were mandated under statute.

○