AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

BEHAVIORAL ADVERTISING: INDUSTRY PRACTICES AND CONSUMERS' EXPECTATIONS

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

JUNE 18, 2009

Serial No. 111–53

Printed for the use of the Committee on Energy and Commerce
energycommerce.house.gov

U.S. GOVERNMENT PRINTING OFFICE
74–087 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
JAN 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 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

JAN 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 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

	Page
Hon. Bobby L. Rush, a Representative in Congress from the State of Illinois, opening statement	1
Hon. George Radanovich, a Representative in Congress from the State of California, opening statement	3
Hon. Rick Boucher, a Representative in Congress from the Commonwealth of Virginia, opening statement	4
Prepared statement	7
Hon. Cliff Stearns, a Representative in Congress from the State of Florida, opening statement	9
Hon. Zachary T. Space, a Representative in Congress from the State of Ohio, opening statement	10
Hon. Joe Barton, a Representative in Congress from the State of Texas, opening statement	11
Prepared statement	13
Hon. Doris O. Matsui, a Representative in Congress from the State of California, opening statement	19
Hon. Joseph R. Pitts, a Representative in Congress from the Commonwealth of Pennsylvania, prepared statement	21
Hon. Phil Gingrey, a Representative in Congress from the State of Georgia, opening statement	23
Hon. Steve Scalise, a Representative in Congress from the State of Louisiana, opening statement	24
Hon. John D. Dingell, a Representative in Congress from the State of Michigan, prepared statement	145
Hon. Edward J. Markey, a Representative in Congress from the Commonwealth of Massachusetts, prepared statement	148
Hon. Anna G. Eshoo, a Representative in Congress from the State of California, prepared statement	150
WITNESSES	
Edward W. Felten, Director, Center for Information Technology Policy, Princeton University	25
Prepared statement	28
Answers to submitted questions	155
Anne Toth, Vice President of Policy, Head of Privacy, Yahoo!, Inc.	36
Prepared statement	38
Answers to submitted questions	158
Nicole Wong, Deputy General Counsel, Google Inc.	48
Prepared statement	50
Answers to submitted questions [1]	
Christopher M. Kelly, Chief Privacy Officer, Facebook	59
Prepared statement	61
Answers to submitted questions	185
Jeffrey Chester, Executive Director, Center for Digital Democracy	68
Prepared statement	70
Answers to submitted questions	189
Charles D. Curran, Executive Director, Network Advertising Initiative	98
Prepared statement	100
Answers to submitted questions	193

[1] Ms. Wong did not respond to submitted questions for the record.

Page

Scott Cleland, President, Precursor LLC 115
Prepared statement 117
Answers to submitted questions [2]

SUBMITTED MATERIAL

Letter of June 16, 2009, from the FTC to Subcommittees, submitted by Mr. Boucher 152

[2] Mr. Cleland did not respond to submitted questions for the record.

BEHAVIORAL ADVERTISING: INDUSTRY PRACTICES AND CONSUMERS' EXPECTATIONS

THURSDAY, JUNE 18, 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 10:08 a.m., in room 2123 of the Rayburn House Office Building, Hon. Bobby L. Rush (chairman of the Subcommittee on Commerce, Trade, and Comsumer Protection) presiding.

Present from Subcommittee on Commerce, Trade, and Consumer Protection: Representatives Rush, Weiner, Matsui, Space, Radanovich, Stearns, Whitfield, Pitts, Terry, Gingrey, Scalise, and Barton (ex officio.)

Present from Subcommittee on Communications, Technology and the Internet: Representatives Boucher, Barrow, Welch, Inslee, Upton, and Buyer.

Staff present: Amy Levine, Subcommittee Counsel; Jen Berenholz, Deputy Clerk; Timothy Robinson, Subcommittee Counsel; Michele Ash, Chief Counsel; Greg Guice, Subcommittee Counsel; Pat Delgado, Chief of Staff (Waxman); Will Cusey, Special Assistant; Sarah Fisher, Special Assistant; Anna Laiton, Counsel; and Roger Sherman, Chief Counsel.

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

Mr. RUSH. Today is a joint hearing of the Subcommittees on Commerce, Trade, and Consumer Protection, and Communications, Technology, and the Internet. And I want to welcome all of you to this hearing. And I want to just give you some advance notice that in about 20 minutes, we will be called to the floor for a series of votes. Some have estimated to be—we are scheduled for about 27 votes on the floor, which is certainly going to extend the hearing, and so we ask that you be patient with us. We will try to conduct this hearing and try to be very mindful of your time, but our actions will be dictated by the House schedule and by the votes on the floor. Now I want to recognize myself for 5 minutes of opening statement. As I indicated, today, the two subcommittees, Commerce, Trade, and Consumer Protection, and Communications, Technology, and the Internet are combining our commitment to privacy and our resources to conduct an extremely important hearing

on Behavioral Advertising: Industry Practices and Consumers' Expectations.

And I just want to take a moment to thank Chairman Boucher for not only his cooperation and working together and teaming up on this particular issue, but I want to thank him also for his past championship and dedication to this very, very important issue. This is but one hearing along a continuum of legislative activity examining the domains of online and off-line consumer privacy and how companies handle and treat consumers' personal information. Most recently, the Subcommittee on Commerce, Trade, and Consumer Protection, which I chair, marked up H.R. 2221, the Data Accountability and Trust Act, a bipartisan bill, which addresses the security of personal information, breaches of that security, and corrects some of the resulting harms to consumers. I am hopeful that there will be more hearings.

There are currently no federal laws specifically governing behavioral advertising nor do we have a comprehensive general privacy law. As members of Congress, we have anticipated for some time that this hearing would be highly informative and very valuable in helping us answer the question that everyone seems to ask, is federal privacy legislation necessary, or should companies be trusted to discipline and regulate themselves? At this hearing, I look forward to hearing from our very distinguished panel of witnesses about this growing trend of online behavioral advertising. Market research firms have estimated that behaviorally targeted ad spending will reach $4.4 billion by the end of 2012. That number is eye-opening as it translates into almost 25 percent of all the online display ad spending that is projected to be spent by year-end 2012.

As prevalent as these ads are becoming, so too are the buzz road, which are purportedly needed to flush out the appropriate contents of fair information principles and practices. Words and phrases such as transparency, choice, notice, consent, consumer expectations, opt-in and opt-out seemingly mean different things to different speakers depending upon an array of variables. Such variables may include the identity of the user, whether he or she has registered with the visited Web site, whether the ads are being served by first or third party sites, the sufficiency and conspicuousness of pre-existing privacy policies and disclosures, the robustness of user-enabled settings for managing user privacy, and the list goes on and on and on and on.

All of these variables are important to consider, but they can muddle the issue of whether legislation is needed. I will be listening intently to your accounts of how up front companies have been about the types of personal information that they are collecting from consumers, what they are doing with the information, and what choices and controls that consumers have over the subsequent use of that information. I want to thank all the witnesses for coming in this morning, for sharing with us, taking away from your busy schedule to provide input, much-needed input, into these matters that are before us today. And I want to thank all the subcommittee members and the staff for so diligently preparing us on this subcommittee for these hearings. And now I want to recognize for 5 minutes for the purposes of opening statement the ranking

member, Mr. Radanovich. Mr. Radanovich is recognized for 5 minutes for opening statement.

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

Mr. RADANOVICH. Thank you, Mr. Chairman, and I want to thank you and Chairman Boucher and my fellow ranking member, Mr. Upton, on these hearings today. I think it is a good issue that we need to be talking about. Privacy continues to be an issue of increasing concern to consumers, and I am pleased that we will be looking at all the relevant issues to determine what the problems are and what possible solutions exist. What was once thought to be an issue limited to business with whom consumers had a customer relationship has been forever altered by the Internet. Progression and innovation in computer and digital technology over the last 20 years has transformed many aspects of our lives, and by the same token that progress has opened the possibility of potential abuses and invasions into our lives.

In the connected world of the Internet where data is instantaneously accessible to anybody in the world, we have learned how vast amounts of sensitive consumer data can be inadvertently disclosed or subject to more malicious and intentional theft. We also know the main reason consumers should be concerned about the amount of personal information out there on the worldwide web is that sensitive personal information can be used for harmful purposes, particularly identity theft. Thankfully, we are addressing some of those concerns with the data security and breach notification legislation moving through the committee right now. Our oversight into the data security issue opened our eyes to the types of sensitive personal information many institutions ranging from businesses to government maintain about us.

While information kept about us may be for legitimate reasons that mandate data retention, for instance, for law enforcement purposes most consumers do not fully understand how information gathered about us will be used or with whom it will be shared. These concerns are legitimate. What is more, these concerns over keeping personal information private are exacerbated by digital technology and the capabilities of Internet technology. Information that filled rooms of file cabinets in a paper-based business can now be stored in devices that attach to a key ring and can be sent over the Internet in seconds, making information theft easy and often untraceable. The ability to instantaneously collect, analyze, and store consumers' online behavior for marketing purposes stretches this dynamic even further.

The Internet quickly evolved beyond its original purpose as a communication tool to become a means of commerce, education, and social interaction. A generation has been raised on the Internet with the ability to find information relevant to their interests and communicate in ways that we could not imagine only 10 years ago, and most expect these services to be customized for their preferences. But many of these technologies and practices that deliver high levels of customization present new challenges and concerns for consumers, primarily understanding what the trade-off is for

these services. Do we need to relinquish personal information about ourselves and our Internet for the purposes of generating more user-specific advertisements in exchange for access to the information we seek on the Internet, and, if so, who has our access to this information?

The Internet has been a successful tool for commerce and has benefitted consumers with convenience, choice, and savings. Relevant advertisements based upon user interests will be more beneficial to the consumer and business, which in concept is no different than the manner in which marketing research determines which advertisements are selected to be placed in magazines, newspapers or on television based on the intended audience. However, in practice the Internet is different because of its ability to track preferences on a minute by minute basis. The question is how advertisers engage in the process of identifying their potential target audience. Specifically, what information is used to generate targeted advertisements? I have a son who I would do anything to protect, and although I cannot monitor him every waking moment and prohibit his ability to access the Internet, nor would I want to, like any parent I want to trust that he will be safe to surf online and interact with his friends without being unknowingly monitored or profiled.

While my son is in a vulnerable demographic millions of Americans of all ages spend time surfing, posting, and shopping on the Internet. How their information is used and what control the individual has over the collection of their information is at the center of the debate of whether we need a federal privacy law, and, if so, how it should be structured and what activities it will address. In the case of my son, I am concerned with the information being gathered and how it is used. I am less concerned with who is conducting the behavioral profiling or what technology they are using. I thank the witnesses today, and I look forward to your testimony, particularly hearing more about what the industry is doing to address many of these concerns in and of itself. Mr. Chairman, I am ready to work with you and the stakeholders to address identified problems and ensure whatever solutions develop will equally apply to the behavior regardless of who engages in it. Thank you, Mr. Chairman.

Mr. RUSH. The chair thanks the gentleman. It is now my privilege and honor to recognize for 5 minutes for the purposes of opening statement the chairman of the Subcommittee on Communications, Technology, and the Internet, the gentleman from West Virginia, Chairman Boucher, for 5 minutes.

OPENING STATEMENT OF HON. RICK BOUCHER, A REPRESENTATIVE IN CONGRESS FROM THE COMMONWEALTH OF VIRGINIA

Mr. BOUCHER. Well, thank you very much, Chairman Rush, and I want to begin this morning by saying thank you to you and to your very fine staff and to Mr. Radanovich from California, your ranking member, as well to Mr. Stearns and his staff for the excellent cooperation we have had among ourselves as the plans for this joint hearing of our two subcommittees have progressed. I very much look forward to our continued collaboration as we consider

the need for legislation and discuss the principles that privacy protection legislation should embody. Broadband networks are a primary driver of the national economy and it is fundamentally in the nation's interest to encourage their expanded use.

One clear way Congress can promote greater use of the Internet for access to information, for electronic commerce, and for entertainment is to assure that Internet users have a high degree of privacy protection, including transparency about information collection practices and uses, and control over the use of the information that is collected from those who use the Internet. I have previously announced my desire to work with Chairman Waxman, Chairman Rush, and ranking members Barton, Stearns, and Radanovich in order to develop legislation this year extending to Internet users the assurance that their online experience will be more secure. Such a measure would be a driver of greater levels of Internet uses, such as electronic commerce, not a hindrance to them.

Today's discussion will examine behavioral advertising and ways to enhance consumer protection in association with it. I am a supporter and a beneficiary of targeted advertising. I would much prefer to receive Internet advertisements that are truly relevant to my particular interests. In fact, I have bought a significant number of items based upon targeted advertising delivered to me from web sites that I frequently visit. And so I have a deep appreciation of the value of targeted advertising from the consumer perspective. It is important to note also that online advertising supports much of the commercial content applications and services that are available to Internet users without charge, and I have no intention of doing anything that would disrupt that very successful, in fact, essential business model for Internet-based companies.

At the same time, I think consumers are entitled to some base line protections in the online space. Consumers should be given clear, concise information in an easy defined privacy policy about what information a web site collects about them, how that information is used, how long it is stored, how it is stored, what happens to it when it is no longer stored, and whether it is ever given or sold to third parties. Consumers should be able to opt out of first party use of the information and for its use by third parties or subsidiaries who are a part of the company's normal first party transactions or without whom the company could not provide its service. All that would fall within the ambit of opt out. Consumers should be able to opt in to use of their information by third parties for those parties' own marketing purposes.

This arrangement should not prove to be burdensome. In fact, it is very much in line with the practices of many, if not most, of the reputable service providers today. I look forward to hearing from your witnesses about their reactions to this arrangement and how it can best balance Internet business models that depend on online advertising with adequate protection for consumers' privacy. For example, have I suggested a workable online opt in and opt out consent arrangement or are there additional situations in which opt out consent might sometimes be appropriate? What safeguards should be in place in order to ensure that consumers are giving meaningful consent to the sharing of their information both on and off the Internet? What role could self-regulatory organizations play

in a statutory arrangement that ensures that all entities that collect information about Internet users abide by a basic set of consumer privacy standards.

I also look forward to learning about emerging approaches to enhancing consumer choice and controlled over the use of information through efforts like the network advertising initiative and persistent opt out cookies. What benefits could these services offer to consumers? What is the best way to inform consumers about the availability of these services and again how should the consumers' meaningful consent be procured? I am also interested in hearing a purview of what the future of behavioral advertising may hold and what services it might enable and how to accommodate privacy concerns associated with those future services. I want to thank our witnesses for taking the time to join us here today. They represent a broad and diverse range of interest and are all deeply knowledgeable about these subjects. We very much look forward to hearing your testimony. Thank you, Mr. Chairman.

[The prepared statement of Mr. Boucher follows:]

STATEMENT OF CONGRESSMAN RICK BOUCHER

Communications, Technology and the Internet and Commerce Trade and Consumer Protection Subcommittee Joint Hearing:

Behavioral Advertising: Industry Practices and Consumers' Expectations

June 18, 2009

Thank you, Chairman Rush.

I appreciate the excellent cooperation among you and I, Mr. Stearns, Mr. Radanovich and our staffs as the plans for today's hearing progressed.

And I look forward to our continued work together as we consider privacy protection legislation over the coming weeks.

Broadband networks are a primary driver of the national economy, and it is fundamentally in the nation's interest to encourage their expanded use. One clear way Congress can promote greater use of the Internet for access to information, e-commerce and entertainment is to assure Internet users a high degree of privacy protection, including transparency about information collection and use practices and control over use of their information.

I have previously announced my desire to work with Chairman Waxman, Chairman Rush and Ranking Members Barton, Stearns and Radanovich to develop legislation this year extending to Internet users the assurance that their online experience is more secure. Such a measure will be a driver of greater levels of Internet uses such as e-commerce, not a hindrance to them.

Today's discussion will examine behavioral advertising and ways to enhance consumer protection in association with it.

I am a supporter and beneficiary of targeted advertising. I would much prefer to receive Internet advertisements that are relevant to my interests. In fact, I have bought quite a number of items that I otherwise might not have purchased as a result of targeted advertising delivered to me by websites that I frequently visit.

It's also important to note that online advertising supports much of the commercial content, applications and services that are available to Internet users without charge, and I have no intention of disrupting this business model.

At the same time, I believe consumers are entitled to some baseline protections in the online space.

- Consumers should be given clear, concise information in an easy-to-find privacy policy about what information a website collects about them, how it is used, how it is stored,

how long it is stored, what happens to it when it is no longer stored and whether it is given or sold to third parties.

- Consumers should be able to opt out of first party use of the information and for its use by third parties or subsidiaries who are part of the company's normal first party marketing operations, or without whom the company could not provide its service.

- Consumers should be able to opt in to use of the information by third parties for those parties' own marketing purposes.

This arrangement should not be burdensome. In fact, it is in line with the practices of many reputable service providers today.

I look forward to hearing from our witnesses about their reactions to this proposal and how we can best balance Internet business models that depend on online advertising with adequate protection of consumers' privacy. For example, have I suggested a workable line between opt-in and opt-out consent, or are there additional situations in which opt-out consent might sometimes be appropriate? What safeguards should be in place to ensure that consumers are giving meaningful consent to the sharing of their information both on and off the Internet? What role could self regulatory organizations play in a statutory arrangement that ensures that all entities that collect information about Internet users abide by a basic set of consumer privacy standards?

I also look forward to learning about emerging approaches to enhancing consumer choice and control over use of information through efforts like the Network Advertising Initiative and the persistent opt-out cookie. What benefits could such services offer to consumers? What is the best way to inform consumers about the availability of such services, and again, how should the consumer's meaningful consent be procured?

I am also interested in hearing a preview of what the future of behavioral advertising may hold—what new services it might enable and how to accommodate privacy concerns.

I thank our witnesses for taking time today to share their views with us about these and other matters.

-###-

Mr. RUSH. The chair thanks the gentleman. The chair now recognizes the ranking member of the Subcommittee on Communications, the ranking member, Mr. Stearns, from Florida. He is recognized 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. Good morning, and, thank you, Mr. Chairman. I also want to echo Mr. Boucher's comment that we look forward to working together in a bipartisan fashion on a very important bill, and I want to thank the witnesses for coming this morning. I think for the most part you are going to educate us. You are the experts here, and we respect your opinions. We want to do no harm here. So I think when you look at the possibility of federal legislation dealing with privacy, we want to make sure that it is consumer centric. Consumers don't care if you are a search engine or a broadband provider. They just want the assurance that their privacy is protected. We must empower them to make these privacy decisions themselves. They feel, they know how much ought to be collected and what should not be collected. Congress cannot and should not make that decision for them, but it can play a role in making sure consumers have the information simply to make their own choices.

That means companies should be as transparent as possible about what information they collect, and, of course, how they are using it. That way consumers will be better able to make informed privacy decisions. This transparency should include robust disclosure and notice outside the privacy policy. Notice and disclosure needs to be clear and conspicuous so the consumers know that. First, some information is being collected. Second, what is the information that is being collected? How is it being used? And, third, how to prevent this information being collected if they so desire. By giving the consumer more robust and transparent information, we can strike the proper balance between privacy protection and strong Internet commerce.

Furthermore, my colleagues, I want to emphasize two principles that should play a prominent role in our examination of this issue. First, we should apply the same privacy standard to companies that are engaged in similar conduct with similar information, but we should avoid applying those same standards to entities that do not use the same types of information for the same purposes and do not have anywhere near the same volume of information about the perspective consumer. For example, search engines in the Internet advertising networks may use a consumer's visit to a particular web site to create profiles not directly related to the reason for the visit. Other entities, like web publishers, collect information only to provide the very service the consumer has come for. Our approach should recognize that.

Second, any legislation in this area should hold various parties accountable only for that which they know and control. We should be wary of efforts to make any one party responsible for the actions of others. Consumers' online activities provide advertisers with valuable information upon which to market their products and their services. Collecting this type of information for targeted advertising

is very important because it simply allows many of these products and services to remain free to consumers. Without this information, web sites would either have to cut back on their free information and services or would have to start charging a fee. Neither result is good for the consumers. Overreaching privacy regulation could have a significant economic negative impact at a time when many businesses in our economy are struggling, so let us be very careful on these issues before we leap to legislative regulatory proposals.

When I was chairman of the Commerce, Consumer Protection, and Trade, I held a number of hearings on privacies. I worked with Chairman Boucher, and we developed a consumer privacy protection at which we dropped as a bill. This bill would have required data collectors to provide consumers with information on the entity collecting the information and the purposes for which the information was being collected. I believe it was, and still is, a good base bill to use as we move forward to develop a new privacy bill. Also, I would like to bring up an issue perhaps that many of us have thought about, and I don't want to bog down our discussion about it. Which agency will regulate and enforce privacy standards? Will it be the FCC or the Federal Trade Commission, a combination or possibly a new agency? I know this issue won't be solved this morning, but it is something we are going to have to work out and work through, and I look forward to doing this in a bipartisan fashion.

And I would be interested, if possible, if some of the witnesses could give us their feelings about how the jurisdiction of this privacy bill would be best supervised with. So, Mr. Chairman, I would conclude by pointing out we have talked a little bit at previous hearings about deep pocket inspection. The point is that whether a company uses deep pocket inspection or reads your e-mail directly, this should be part of the privacy rules in some way. So I think our witnesses can also help us on that particular aspect, so I look forward to hearing and thank you for the opportunity to speak.

Mr. RUSH. The chair thanks the gentleman. The chair now recognizes the gentleman from Ohio, Mr. Space, for 2 minutes for the purposes of opening statement.

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

Mr. SPACE. Thank you, Chairman Rush and Chairman Boucher, Ranking Member Radanovich and Ranking Member Stearns for convening us today on the topic of behavioral advertising. I was struck when reviewing Professor Felten's testimony by a comment that he makes, "Responsible ad services typically collect less information and track users less intensively than the technology would allow." To me, this means that just because we can doesn't mean that we should. I certainly understand the need for companies to advertise on their sites. Doing so is what enables our constituents to access free content, products, and services on line. They also understand the desire of ad companies to supply consumers with ads that are of more relevance to them. This is a better business model for the companies and potentially a service to consumers.

However, I want to make clear that one bad apple could spoil the whole bunch here. The moment online consumers believe their per-

sonal information is at risk of corruption, misuse or theft will be the moment this approach we are discussing today will cease to work. I strongly believe it is in the interest of all parties to disclose to consumers their advertising practices and intent and to ensure that consumers' personal information is strictly guarded against security breaches and exploitation. I look forward to these conversations today and to working with my colleagues on this issue as we move forward. I yield back my time.

Mr. RUSH. The chair thanks the gentleman. It is now my pleasure and honor to recognize for 5 minutes for the purposes of opening statement the ranking member of the full Committee on Energy and Commerce, Mr. Barton, is recognized for 5 minutes.

OPENING STATEMENT OF HON. JOE BARTON, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TEXAS

Mr. BARTON. Thank you, Mr. Chairman. As I look on the other side of the aisle, I am glad to see that none of the Democrats who played on the Democratic baseball team are actually in the room, so I can congratulate them in their absence and I won't have to do it face to face when I see them on the floor. But last night Mike Doyle, who is the manager of the team, Bart Stupak, who is on this committee, played an amazing game. It wasn't their usual Democratic bumbling error game. They actually played very well as a team, and as a result they beat the stalwart Republicans 15–10. John Shimkus, who is our starting pitcher, played an excellent game, and we had a number of Energy and Commerce Republicans, Mr. Gingrey, Dr. Gingrey, who is here, walked at a key time and later scored.

Mr. Scalise, who is here, played second base some and also did some base running and scored. Mr. Pitts, who came out and watched the game, and luckily didn't try to play although we could have used his bombing skills from the Vietnam War. So, anyway, we raised quite a bit of money for charity and had a good time. When you all see Mike Doyle and you see that he is grinning from ear to ear just congratulate him and tell him to take pity on the downtrodden Republicans who didn't quite have the stuff last night.

On this hearing, Mr. Chairman, I do want to thank you, thank Mr. Boucher, Mr. Stearns, Mr. Radanovich for working in a bipartisan fashion to protect the privacy and security of every American's personal information. I am glad that we are working on this in a bipartisan way. I especially appreciate Chairman Rush's agreement to act on the Republicans' data security bill. That bill has implications for the broader privacy discussion, and I hope that that bill will move forward in the full committee. Along with Congressman Markey, I co-chair the Congressional Privacy Caucus, so I am glad that we are working on these issues in a bipartisan way. I, myself, every few days hit the delete button and clean out all the various cookies on the computer and at my home. It is amazing to me how many of those accumulate and most of the time without absolutely any knowledge of myself or anybody else for that matter that they are being put on our computer.

I think it is a big deal if somebody tracks where you go and what you look at without your personal approval. We wouldn't like that

in the non-Internet world, and I personally don't like it in the Internet world. The information about myself is mine. Unless I choose to share it, I would just as soon that it stay my information only. I think that I have the right to know what information people are gathering about me and the right to know what they are doing with it. It is obvious that the public agrees with the statement that I just made because poll after poll shows that they think that their information and their right to privacy is just as important on the Internet as it is in the non-Internet world. When I open an e-mail for the new Dallas Cowboy Stadium that is in my congressional district, I don't expect to begin receiving unsolicited ads for airlines tickets to the Dallas-Fort Worth area or hotels, also in my district in Arlington, Texas.

It is obvious that people track what I do and where I go, and try to take advantage of that. Fortunately, technology has come quite a ways in protecting the individuals. We started looking at the spyware problem back in the 107th Congress, and thanks to the work among others Congresswoman Mary Bono Mack, Ed Towns, Chairman Dingell, those spyware infections are not near the problems that they used to be. However, today companies continue to gather, maintain, and use data through a variety of technological methods. Some of those companies such as Verizon and Comcast are large companies. They are regulated in some parts of their business model, and I think they are trying to act appropriately. There are other companies, so-called ISP locators, that I personally don't even know their name. Then you have the in-between companies, the so-called edge companies like Yahoo! and Google. Put together, it still is a little bit of a wild west out there, and I think it is time that Congress begin to look at and try to bring some law and order to that particular wild west area.

I see that my time has expired, Mr. Chairman, so I will submit the rest of the statement for the record. Suffice it to say that I am glad that you and Congressman Boucher are working with the Republicans and taking a serious look at this. I also want to commend the private sector that is here today. It is my understanding that you are working together to come up with some voluntary rules, and it is always preferable in my opinion to do it through a voluntary market-based approach as opposed to a mandatory regulatory approach. So in any event again thank you, Mr. Chairman, and once again congratulations to the Democrats for winning the baseball game last night. I yield back.

[The prepared statement of Mr. Barton follows:]

Statement of the Honorable Joe Barton
Ranking Member, Committee on Energy and Commerce
"Behavioral Advertising: Industry Practices
and Consumers' Expectations"
June 18, 2009

Thank you, Mr. Chairman, and thank you for holding this hearing.

I want to say a word about the good deeds that Chairman Boucher, Ranking Member Stearns, Chairman Rush, and Ranking Member Radanovich are doing to protect the privacy and security of people's personal information. This committee has a long history of examining these issues and doing something useful once we get the facts in hand, and I'm glad we're continuing that tradition in a bipartisan way. A pertinent example is the fact that Mr. Rush's subcommittee acted on the Republicans' old data security bill. That bill has implications for the broader privacy discussion, and I look forward to moving on that in the Full Committee.

I co-chair the Congressional Privacy Caucus because I think it's a serious issue. In fact, every couple of days I clean out the "cookies" on every computing device I own. The Internet a lot of propagates mischief as well as knowledge, and plenty of what happens there goes on without the everyday user being aware of it. Loss of their personal privacy, however, is a big deal for most Americans, and it's a very big deal to me. My information is mine. I have the right to know exactly what information people are gathering about me and exactly what they are doing with it. In fact, I think people should have the option to prevent any kind of data collection in the first place.

The public calls for action have reached a deafening pitch, and that's a big part of why we're here today. People everywhere are deeply troubled by what's going on. When you open an email that says, "Dallas Cowboys" and "unbelievable new stadium," and then begin receiving unsolicited ads for airline tickets to DFW and

hotels in Arlington, Texas, you realize that somebody has been watching.

Technology has come a long way in helping users. When we started looking at the spyware problem back in the 107th Congress, we found that the world of Internet advertising was a Wild West where might made right. There was neither a lawman in town nor any laws to enforce. I'd be remiss if I didn't mention Mary Bono Mack's great work over the years on that issue. Thanks to her efforts along with Ed Towns, Chairman Dingell and others, spyware infections are now a fading worry.

Yet today, many companies gather, maintain, and use data about their users or customers using a variety of technological methods. Some companies are regulated carriers such as Verizon or Comcast. Other companies are so-called "edge" companies like Yahoo! Or Google. Some folks do all this collection and analysis within their own company, and others use joint partnerships or contract with third parties.

I hope that we can all agree that regardless of the regulated status of a company or the specific data-gathering technology that a company is using, our policy focus should be remain on the protection of American's privacy. Thus, good public policy in my mind would be technologically neutral, and it would not inadvertently create comparative advantages between companies based on regulated status or different data-gathering techniques.

Mr. Boucher and Mr. Rush have indicated that they want to move forward with privacy legislation that would lay out some strict rules in this area, and I look forward to working with them.

It's also my understanding that the industry, both carriers and edge companies, is engaged in a serious effort to put together its own rules to address privacy concerns by being more transparent about practices, offering more choice to users, and better educating people about online activities.

I applaud that effort—responsible companies taking the initiative to do the right thing should be always encouraged. And

as a Republican, I believe that the heavy hand of regulation should only be used to correct market failures that companies are unable or unwilling to address.

As we begin to work on legislation, we should take care not to do anything that would discourage or render useless the self-regulatory effort of responsible industry companies to do the right thing, and I encourage all those involved in this industry process to move forward quickly with strong consumer protections and the most clear and transparent policies that are technologically possible. And I want to reiterate that I expect companies, regardless of regulated status or what specific technologies or business models they employ to gather information, to be held to the same standards when it comes to protecting consumer privacy. I would hope that the industry would keep that thought in mind as they work on their own ways to promote privacy protection and protect consumers from abusive practices.

I want to thank our expert witnesses for making the time to participate and inform our process. This isn't an easy task, and we'll need the stakeholders in industry and in the advocacy community to help us.

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

\

Mr. RUSH. The chair thanks the ranking member. It is now my honor to recognize the gentle lady from California for 2 minutes for the purpose of opening statement, Ms. Matsui.

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

Ms. MATSUI. Thank you, Mr. Chairman. I want to thank you and Chairman Rush for calling today's joint hearing and applaud both your leadership in addressing this important issue. I would also like to thank our panelists for being here with us this morning. Today, we are here to examine the practices and consumer protections from a growing online advertisement practice known as behavioral advertising. As broadband access continues to expand across the country, more and more Americans rely on the Internet for news information, online videos, and to purchase goods and services. Americans need to have trust and confidence that their personal information are properly protected. Privacy policies and disclosures should be clear and transparent so consumers can choose what information they want to view and receive on the Internet instead of inappropriate collection and misuse of their 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 are comfortable with using the Internet and know with confidence that meaningful privacy safeguards are in place or ensuring that we don't stifle innovation. I thank both of you, Mr. Chairman, for holding this important hearing today, and I yield back the balance of my time.

Mr. RUSH. The chair thanks the gentlelady. Now the chair recognizes the gentleman from Kentucky, Mr. Whitfield, for 5 minutes for the purpose of opening—let me correct that. The chair recognizes the gentleman from Michigan.

Mr. UPTON. I thank my friend, and I will not take my 2 minutes. We have great attendance. We will see what the attendance is after lunch when we return after these votes. I would like to associate myself with Mr. Barton's remarks. The information is yours. When you make a phone call, no matter who it is, you don't expect AT&T or Verizon to share the information with somebody else. You can imagine if you ordered a pizza on the phone and all of a sudden you get different pizza companies coming in knowing that you are going to be subscribing to that. That information is personal. It shouldn't be shared unless that individual allows and knows that it is going to be shared. It needs to be protected. It is nobody's business. You don't expect to have someone follow you in your car when you go make an errand whether it be to a dry cleaner or wherever you might go and expect some competitor then to perhaps get the information to trace you back. So this is a great hearing, and I look forward to it and I yield back the balance of my time.

Mr. RUSH. The chair thanks the gentleman. The chair now recognizes the gentleman from Georgia, Mr. Barrow, for 2 minutes for the purpose of opening statement.

Mr. BARROW. I thank the chairman. I am going to waive opening but I want to thank the ranking member for his kind words of congratulations. In solidarity with Mr. Pitts, I want to remind the ranking member that those of us who sit in the stands and cheer also serve. Thank you very much.

Mr. RUSH. The chair now recognizes the gentleman from Kentucky, Mr. Whitfield, for 5 minutes.

Mr. WHITFIELD. Thank you, Mr. Chairman. We certainly appreciate all these witnesses being here today as we explore this very important subject. As online communities use an array of sophisticated and ever evolving data collection and profiling applications, it is important that we focus on protecting privacy. Today, I think we will be hearing about privacy policies at various companies, the data retention that they do, and as we proceed and think about legislation, it is imperative that we use a balanced approach and proceed with caution. And I think if we do have any legislation it certainly should apply equally to all entities throughout the Internet ecosystem, and I will yield back the balance of my time.

Mr. RUSH. The chair now recognizes the gentleman from Ohio, Mr. Pitts from Pennsylvania, Mr. Pitts, recognized for 2 minutes.

Mr. PITTS. Thank you, Mr. Chairman. I worked real hard on an opening statement, but I think I will submit it for the record. Just let me say I believe that consumer privacy rights should be carefully guarded. I am also encouraged by private industry's recent steps to further protect consumers. It is my hope that if legislative action is taken that we will do so in a careful manner striking a delicate balance between the necessary steps we must take to protect consumers, and the ability for industry to continue to be successful. So with that, I will submit the rest for the record and yield back.

[The prepared statement of Mr. Pitts follows:]

Opening Statement of Mr. Joe Pitts for the Commerce, Trade, and Consumer Protection Subcommittee Hearing:

Behavioral Advertising: Industry Practices and Consumers' Expectations

June 18, 2009

Thank you, Mr. Chairman, for holding this important joint hearing to examine the potential privacy implications of behavioral advertising.

Website operators utilize online advertising to generate the revenue needed to support their businesses. This allows consumers to read, watch videos, and utilize social networking services without charge.

Behavioral advertising, or tracking of consumers' online activities in order to deliver tailored advertising, allows businesses to align their ads more closely to the inferred interests of their audience.

This practice has raised privacy concerns as consumers do not necessarily understand, or, in some cases, control, what information is being collected about their preferences and what information is being shared.

These concerns have led industry to recently enact privacy standards on their own volition. Today, we are examining whether or not the federal government needs to take further action in this arena.

As this committee contemplates legislative action, I think we must keep in mind that internet advertising allows many small business owners to flourish. I recently met with one gentleman and his wife who were able to live in a rural area and home school their children because of the money they made from the advertising on their small business website.

Interactive advertising is also responsible for $300 billion of economic activity in the U.S., according to a new study. This is approximately 2.1% of the total U.S. (GDP). If the federal government unduly restricts this industry, it will have an enormous impact on our economy—and economy that is struggling for its livelihood.

I believe that consumers' privacy rights should be carefully guarded. I am encouraged by private industries recent steps to further protect consumers.

It is my hope that if legislative action is taken, we will do so in a careful manner—striking a delicate balance between the necessary steps we must take to protect consumers and the ability for industry to continue to be successful.

I look forward to hearing from our witnesses. I yield back.

Mr. RUSH. The chair thanks the gentleman. The chair now recognizes the gentleman from Georgia, Dr. Gingrey, for 2 minutes for the purpose of opening statement.

OPENING STATEMENT OF HON. PHIL GINGREY, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF GEORGIA

Mr. GINGREY. Chairman Rush and Chairman Boucher, Ranking Member Radanovich and Stearns, I want to thank you for calling this hearing today on the emerging use of behavioral or interest-based advertising online. This type of advertising only represents a small portion of all online ads. By 2012 this type of advertising is estimated to reach $4.4 billion in revenue. Therefore, it is important for these subcommittees to take a further look at this industry in order that we ensure the online privacy of consumers. When hearing testimony from this panel today, I believe that it will be important that we focus on three components of any potential regulation that these subcommittees propose. First, it is important to distinguish what it is that we are going to be regulating.

Currently, most interest-based advertising is conducted through the use of web browser cookies. These encoded text files help indicate a user's online activity, thereby enabling advertisers to customize ads based on a series of preferences. However, as we have seen in the IT industry, particularly over this last decade, technology moves very quickly and if we are to propose regulations for this industry then we must make the determination of exactly how and what we are going to regulate.

Mr. Chairman, we must also examine which federal agency would be best suited to coordinate any potential regulation. Both the Federal Communications Commission, FCC, and the Federal Trade Commission have jurisdiction over elements of behavioral advertising. Therefore, for the sake of consumers if regulations are necessary, we must coordinate the efforts and responsibilities of these two governmental entities, thereby allowing for industry growth while at the same time safeguarding an individual's private information. Lastly, Mr. Chairman, we would also have to determine whom we would be regulating. Would it be the Internet service provider or the advertisers or the web interfacing companies represented here today?

Accordingly, I think it will be important that as we move forward, we diligently take the time to hear from ISP companies and advertisers as a way to give us different perspective on this important issue that will continue to be crucial to the further development of online activity. Mr. Chairman, the heart of this hearing is the American consumer so our focus must be their overall protection. I look forward to hearing from the panel, and 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 for the purposes of opening statements.

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

Mr. SCALISE. Thank you, Mr. Chairman. I want to thank you and the ranking members of the subcommittees for having this hearing on behavioral advertising. I am pleased that both subcommittees are examining this issue as well as the greater issue of data privacy. I know that Congress and this committee have held hearings on data privacy in the past, but as we know technology continues to advance and develop in ways that provide tremendous benefits to consumers. But these advancements and benefits can expose consumers to certain risks. Therefore, we must continue to examine ways to ensure consumers don't have their personal information compromised. The technology industry is one of the most advanced and competitive industries in our country. It is also one of the most beneficial, both for consumers and for our economy.

We are able to share information, exchange ideas, and conduct commerce in ways that were never imagined just a few decades ago. The industry also provides millions of good high-paying jobs for people all across this country. One thing that I think must be pointed out is that the industry has evolved and grown on its own with little regulation from the federal government. Some would say that the government's failure to regulate this industry is one of the reasons it has grown and provided so many good jobs. Yes, there have been bad actors in the industry, and there are issues we must address in protecting consumers' personal information, but I would hope we would proceed with caution when stepping in or when drafting legislation in this area. 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 to do that.

I hope today's hearing does not focus on how the government can improve the industry. As we continue to delve into this issue today and future hearings, we should focus on the consumer and what will offer consumers the greatest transparency into the online practices and give them meaningful control over their personal information. For this reason, I believe that self-regulation is sufficient and if privacy regulatory requirements are needed, they should be consistent across the industry and not be greater for one technology compared to another. Everyone involved in online advertising, ISPs, search engines, advertising networks, web site publishers and others, should all be subject to the same requirements, and Congress should not try to pick winners and losers. After all, consumers are not always aware that their Internet activities are being tracked.

They care about what information is collected and what it is used for. They want to know if this is going on and, if so, they should be able to opt out if they so choose and be assured that a breach of their personal information will not occur. I look forward to the hearing and the comments from our panelists today, particularly on self-regulation and what changes they will make to ensure protection of personal information and what changes they plan on making moving forward. It is important that these committees and subcommittees understand their positions and activities as well as

all the implications of these new advertising practices. Thank you, and I yield back.

Mr. RUSH. The chair thanks the gentleman. As I indicated earlier, there is a vote occurring on the House floor. It is a series of votes, and so we will recess the committee until the completion of those votes, and we will reconvene 15 minutes after the completion of those votes. The committee now stands in recess.

[Recess.]

Mr. RUSH. The committee will reconvene. I certainly want to thank each and every one of you for your patience. I want to also apologize for the time that you have been forced to spend here. This has been an abnormal day with a lot of abnormal activities, and I might add it has been a record-breaking day. According to some, we have had at least 54 consecutive votes one after another and this never happened before that we know. So it is not something we are proud of, but it has been that kind of a day. We are going to proceed right to our witnesses.

Starting on my left, to the right we will proceed with introducing our witnesses. Mr. Jeffrey Chester is the Executive Director for the Center for Digital Democracy—let me start over again. Mr. Edward W. Felten is Professor of Computer Science at Princeton University. Next to Mr. Felten is Ms. Anne Toth. She is the vice president of Policy, Head of Privacy for Yahoo. Ms. Nicole Wong is the Deputy General Counsel responsible for privacy for Google. Mr. Christopher M. Kelly is Chief Privacy Officer at Facebook. Mr. Jeffrey Chester is Executive Director for the Center for Digital Democracy. Mr. Charles D. Curran is the Executive Director of Network Advertising Initiative. And Mr. Scott Cleland is the President of Precursor LLC. Again, we want to thank the witnesses for their patience and for their appearance before the subcommittee. It is the practice of this subcommittee now that we will swear in all the witnesses, so would you please stand and raise your right hand?

[Witnesses sworn.]

Mr. RUSH. Let the record reflect that all the witnesses have responded in the affirmative. Now we will ask the witnesses to enter into opening statements. And, Mr. Felten, you are recognized for 5 minutes or thereabouts. So please pull the mike in front of you, turn it on, and let it rip. Thank you.

TESTIMONY OF EDWARD W. FELTEN, DIRECTOR, CENTER FOR INFORMATION TECHNOLOGY POLICY, PRINCETON UNIVERSITY; ANNE TOTH, VICE PRESIDENT OF POLICY, HEAD OF PRIVACY, YAHOO!, INC.; NICOLE WANG, DEPUTY GENERAL COUNSEL, GOOGLE INC.; CHRISTOPHER M. KELLY, CHIEF PRIVACY OFFICER, FACEBOOK; JEFFREY CHESTER, EXECUTIVE DIRECTOR, CENTER FOR DIGITAL DEMOCRACY; CHARLES D. CURRAN, EXECUTIVE DIRECTOR, NETWORK ADVERTISING INITIATIVE; AND SCOTT CLELAND, PRESIDENT, PRECURSOR LLC

TESTIMONY OF EDWARD W. FELTEN

Mr. FELTEN. Thank you, Chairman Rush, Chairman Boucher, for the opportunity to testify today. My name is Edward Felten. I am a Professor of Computer Science and Public Affairs at Princeton

University. I am here as a technologist. I am a computer science professor and I would like to explain some of the technology behind behavioral advertising. The most serious privacy concerns are raised not by the presence of advertising but by the gathering of information about users that can be used either to target ads or for other purposes. I would like to describe what technology makes possible. Responsible ad services do not do everything that is possible, and I don't mean to imply otherwise. Others on the panel can describe what their own systems do do.

To explain what this technology allows, I would like to walk through a scenario illustrated by the diagram on the last page of my written testimony. And if I could have the display, please, of the Power Point. What I would like to describe, Mr. Chairman, is a scenario involving behavioral advertising. In the beginning of the scenario, I go to a weather site, and I look up Thursday's forecast for Washington. The weather site sends me a page with the forecast information and a hole where the ad should be. And along with that page it sends my computer a command telling it how to find the ad. Following these instructions, my web browser connects to an ad service shown here at the bottom and asks for an ad.

Along with this request, information is sent to the ad service about me, the fact that I am looking up Thursday's forecast for Washington and the fact that I normally look up the forecast in Princeton, New Jersey. The ad service remembers this information. The ad service sends an ad, which is inserted into the page. The service also sends an ad in this case related to travel to Washington because I looked up the Washington, D.C. forecast. The service also sends along its so-called cookie which contains a small, unique code which in this example in the diagram is 7592, and my computer stores this cookie. Later, I visit a social network page which also contains an ad. Again, the page has a blank space for the ad and my computer contacts the ad service to get an ad.

My computer automatically sends along the cookie that the service provided earlier. This request for an ad carries more information about me. It says that I am interested in baseball and jazz, which the social network site knows, and that my name is Edward Felten. The ad service recognizes that the cookie is the same as before so it knows that I am the same person who looked up D.C. weather earlier and it adds the new information to its profile of me. The service sends back an ad. This time it is an ad for Washington Nationals tickets because I looked up Washington weather earlier, and I am interested in baseball.

Notice that the ad service is connecting the dots between things that I did on different sites between something I did on the weather site and something I did on the social network site. This allows it to better target ads and also to build up a more extensive profile about me. Next, I go to a book store and look up books about travel in Hawaii. The book store site sends this information to the ad service along with another ad request. Again, the cookie allows the ad service to link together my book store activities with my earlier activities on other sites. The ad service sends back an ad for jazz CDs because it knows I like jazz because the social network site told it. By this point, the ad service knows enough to identify me. It knows I live in Princeton and it knows that my name is Edward

Felten. The ad service buys access to a third party commercial database using what it knows about my identity to get more information about me.

In this example, the ad service gets my credit report in by insurance history, which it adds to my profile along with the other information it had. And, finally, I go to a news site that uses the same ad service. My computer again requests an ad. The ad service in this case sends an ad for budget Hawaiian vacations. It knows that I am interested in visiting Hawaii because I looked at Hawaii books at the bookstore, and it knows I am interested in a low cost trip because it has my credit report. The news site sends information about what I was reading. In this example, I was reading about cancer treatments. This information is added to my profile as well.

In this scenario, the ad service got information in three ways. First, content providers sent along information about what I was doing on their sites and what I had done in the past. Second, the ad service connected the dots to link my activities across different sites at different times. And, third, the ad service accessed third party commercial databases. All of this information ended up in my profile. The result was well-targeted ads but also the creation of an electronic profile of me containing sensitive information which could in principle be resold or reused for other purposes. Now ad services are not the only parties who can assemble such profiles but large ad services do have a prime opportunity to build profiles due to their relationships with many content providers who can pass along information about users, and due to the ad service's ability to connect the dots by linking together a user's activities across different web sites.

All of this is possible as a technical matter which is not to say that responsible ad services do all of it or even most of it. Ad services may be restrained by law, by self-regulation or by market pressures. What is clear is the technology by itself cannot protect users from broad gathering and use of information.

Mr. RUSH. Mr. Felten, I am embarrassed to say this, but would you please bring your statement to a close? You have extended your time.

Mr. FELTEN. Thank you, Mr. Chairman. I was just wrapping up. I just wanted to thank the committee for holding this hearing and for giving me the opportunity to testify. Thank you.

[The prepared statement of Mr. Felten follows:]

Testimony of Edward W. Felten
Professor of Computer Science and Public Affairs, Princeton University

United States House of Representatives, Energy and Commerce Committee
Subcommittee on Communications, Technology and the Internet, and
Subcommittee on Commerce, Trade, and Consumer Protection
Hearing on
Behavioral Advertising: Industry Practices and Consumers' Expectations
June 18, 2009

Chairmen Boucher and Rush, Ranking Members Stearns and Radanovich, and members of the committees, I thank you for the opportunity to testify about the technology behind behavioral advertising.

My name is Edward W. Felten. I am a Professor of Computer Science and Public Affairs at Princeton University. I also serve as the founding Director of the Center for Information Technology Policy, an interdisciplinary research and teaching center at Princeton that focuses on public policy issues relating to computers and the Internet. My primary background is in computer science, and my main subfields of computer science include computer security and privacy, and Internet technologies. I have served as an advisor or consultant to the U.S. Departments of Defense, Homeland Security, and Justice, and the Federal Trade Commission. I have testified twice previously before House hearings and once before a Senate hearing. I am a Fellow of ACM, the leading professional society for computer scientists, and I serve as Vice-Chair of USACM, which is ACM's U.S. Public Policy Council.

I have been asked to testify about technical aspects of behavioral advertising, such as how online ads are delivered, and how information can be gathered and used by ad services. In discussing these topics, it is important to distinguish between what the technology allows, and what ad services actually do. Responsible ad services typically collect less information, and track users less intensively, than the technology would allow. I will describe what is possible technically, and I will leave it to other witnesses to describe which of these technical possibilities their services exploit.

1. Ads and Privacy

The most serious privacy concerns are raised not by the presence of advertising, but by the gathering of information about users that can be used either to target ads or for other purposes. The same kind of information-gathering can and does occur in contexts other than advertising. Regardless of when, where, and how information is gathered, there is no *technical* barrier to the resale of that information into secondary markets, or to the reuse of the information for other purposes. Accordingly, my technical discussion will be in the context of advertising, but it will be concerned mostly with how information about users can be gathered and used.

2. How Online Ads are Delivered

A typical online advertising scenario involves four parties. A *user* views a web page created by a *content provider*. The content provider leaves a space on the page for an ad, and an *ad service* chooses an ad to fill that space. An *advertiser* pays the ad service to place its ads, and the ad service pays the content provider for providing space.

Although the user sees the content and the ad together, they typically come from different places. The user's computer fetches the content, which has a blank space where the ad will be. The content comes with instructions that tell the user's computer where to go to get the ad, and where the ad should be placed on the page. The user's computer, following these instructions, connects to the ad service and asks it to provide an ad. The ad service decides which ad to provide; the chosen ad is delivered to the user's computer where it is displayed. Notably, the content provider and the ad service need not, and often do not, communicate directly during this process. Instead, the content provider simply causes the user's computer to fetch and display an ad from the ad service.

3. How Ad Services Gather Information

The ad service can increase the effectiveness of the ads it places, and thereby increase its revenue and the revenue of the content provider, by placing ads that are especially likely to be interesting and relevant to the user. Ads can be targeted based on context, on the user's past behavior, or on other information known about the user. For example, I might be shown ads for baseball tickets because I am reading a page about baseball, or because I recently purchased a baseball glove from a sports web site, or because the ad service knows that a sports magazine is regularly delivered to my home address. In general, the more information the ad service has about the context and the user, the more precisely it can target ads. Thus ad services have a natural incentive to collect and use detailed information about users.

Ad services can acquire information in three basic ways: they can get information from content providers, they can link users' activities across multiple sites, and they can use third-party commercial databases.

A. Getting Information From Content Providers

Ad services' first source of information is the content provider, which can supply information about the user, or about what the user is doing. For example, suppose I am viewing a newspaper story that is shown with a banner ad. The content provider (in this case, the newspaper) can tell the ad service anything it knows about me, including information that I provided when I signed up for an account with the content provider: it can reveal that I am male; or that I am a male in his forties living in New Jersey; or that I am a 46-year-old male, married with children and living in the 08540 area code; or that I am Edward W. Felten of Princeton, New Jersey, credit card number _____. Similarly, the content provider can supply the ad service with information about my interests: that I tend to read about national news, technology, and sports; that I read more about baseball than about hockey; that I often read Los Angeles Dodgers box scores; or (hypothetically) that I have recently shown interest in stories about cancer treatments.

In addition to information about the user generally, the content provider can supply information about what the user is doing at the moment. For example, a newspaper site might tell the ad network which story I am currently reading, or a travel site might tell the ad network that I am currently shopping for a train ticket to Washington.

The technical mechanism for passing this information from content provider to ad service is straightforward. Recall that when the content provider sends a web page to the user's computer, the page comes along with a command which the user's computer will carry out to request an ad from the ad server. The content provider can attach information to this command, and the ad service can retrieve that information when it receives the command. Additionally, information can be passed directly from the content provider to the ad service, through a back channel rather than going through the user's computer. In principle, any information known to the content provider can be provided in this way.

In some cases, the content provider may be the same organization as the ad service, or they may have a common corporate parent. For example, Facebook may serve ads for placement on content pages provided by Facebook itself; or Doubleclick, which is owned by Google, may serve ads on content pages provided by Google. In such cases, information might flow more easily from the content provider to the ad service, although the company may choose to impose internal controls on such flows, or even to maintain a strict "Chinese wall" between its content provider and ad service components.

B. **Linking Users' Activities Across Multiple Sites**

The second way an ad provider can gather information is by linking together actions by the same user across different web sites. In the course of a week I may visit many sites that show ads from the same ad service. If the ad service can determine that all of these visits came from the same person, then it can link together the information it gets from those visits, to create a more complete picture of who I am and what my interests are. For example, suppose I go to a social network site to discuss baseball, and that site uses a particular ad service. If that ad service knows that I am the same person who previously visited a weather site to look up Thursday's weather forecast for Washington, then the site can place on the social-network page an ad for tickets to a Washington Nationals game. This is possible because the ad service can link together the fact that I checked the Washington weather forecast on one site yesterday, with the fact that I discussed baseball on a different site today.

Of course, the information that is linked might be much more sensitive. For example, suppose (hypothetically) that last week I visited a news site and read several stories about cancer treatments. If the ad service can tell that the person who read this cancer information is the same person who checked the weather forecast and joined the baseball discussion, then it can add the (hypothetical) cancer information to its profile of me.

Further, if the ad service is able to link this information to another action that it knows was taken by Edward W. Felten of Princeton, New Jersey, such as a credit card transaction, then it will know that all of these actions were taken by me. The ad service could associate my cancer-related reading with my true name and identity, even if the website where I read the cancer stories did not know or reveal my identity.

There are several technical mechanisms that services can use to link together visits by a single user to different sites at different times. The most common such mechanism involves web "cookies." When the browser on a user's computer interacts with a service across the Internet, standard web technologies allow the service to provide a small piece of information, known as a cookie, that will be stored on the user's computer. Later, whenever the same browser re-connects to the same service, the browser will give the service a copy of the cookie. Services often give computers a cookie containing a unique number; if the same computer connects to the same service again, providing a copy of the cookie, the service can use the unique number to recognize that it has seen this computer before.

If an ad service can link together my various online activities, and if the ad service remembers all of the information about me that content providers have passed along, then the ad service can build up a profile of my online activities and interests. If any of the content providers passed along personally identifying information sufficient to convey my real-world identity, then the ad service will be able to connect its profile of my online activities to my real-world identity. There are no *technical* barriers to the ad service selling this information to third parties.

C. Using Third-Party Commercial Databases

The third way an ad service can gather information for targeting ads is by buying information from third-party providers such as consumer information databases. This is possible if the ad service knows the real-world identity connected to the online activities. 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.

Of course, the fact that something is possible as a technical matter does not imply that reputable ad services actually do it. In practice, information gathering by ad services may be restrained by law, by self-regulation, by social norms, or by market pressures such as the desire of users to avoid sites that carry privacy risks. Services may choose not to gather, or not to use, certain kinds of information, or to gather and use only information that is less specific or less sensitive. I will leave it to other witnesses to describe the practices of their companies.

4. Web Beacons: Tracking Without Ads

Behavioral tracking can also happen on its own, without any advertisements. In this case, the same kind of cookie system is used to track user behavior and interests, just without displaying an ad. The data is still gathered, and it can still later be used to target future ads, or for any other purpose. When the tracking happens on its own, without any ad being displayed to the user, the tracking code is known as a "web beacon."

From the ad service's standpoint, a web beacon has the information-gathering power of an ad, but of course it lacks the ad content. The ad service can still use the information gathered by the beacon to build up its profiles about users, in order to improve ad targeting to those users later.

From the user's standpoint, though, the experience is very different: a web beacon, unlike an advertisement, leaves no outward mark on the web site the user sees. (Technically sophisticated users, or simple software, could find the beacon by examining the web page's code, but few users will do this.) As a result, users who wish to avoid being tracked will not know there is anything to opt out of, even if the ad network or other service that has placed the beacon does offer an opt-out mechanism.

5. Self-Help by Users

Users who are willing to engage in self-help, in an attempt to stop ad services from tracking them, have a limited ability to do so. Users have two main self-help strategies: they can try to block ads entirely; or they can try to stop ad services from linking together their actions across web sites.

A. Blocking Ads Entirely

The first self-help strategy tries to block ads entirely. This requires more than simply blocking visual presentation of ads. If the goal is to prevent ad services from gathering information about the user and his activities, then the user must prevent his computer from communicating with ad services. The typical approach is to establish a blacklist containing the network addresses of known ad services, and to prevent the user's browser from connecting to addresses that are on the blacklist. If the user's browser never connects to an ad service, then the ad service does not see what the user is doing and cannot link together the user's actions across different web sites.

If adopted widely, ad-blocking could potentially endanger the business models of content providers who rely on advertising revenue. Today, relatively few people use ad blockers. There are technical countermeasures that ad services could adopt, in an effort to defeat ad-blockers, but these countermeasures would be only partially successful.

It would be possible, in principle, to create an ad blocker that allowed ads from services that complied with certain specified privacy guidelines, while blocking ads from other ad services. This could give content providers a way to get some ad revenue, while protecting users against some privacy risks. Doing this would require relatively straightforward technical modifications to existing ad blocking tools.

B. Stopping Ad Services

The second self-help strategy tries to stop ad services from linking together the user's actions across different web sites. These approaches mainly revolve around controlling web cookies. Recall that ad services often use cookies to place a unique mark on a particular user's computer, so the ad service can recognize the same computer later (and can infer that that computer is likely under the control of the same user). By erasing an ad service's cookie, the user can try to stop the ad service from connecting new actions to the user's previous history. In addition, most current browsers provide some kind of "anonymous browsing mode" (or similarly named feature) in which the browser tries to avoid giving content providers any clues about the user's past browsing history. The theory is that anything the user does while in anonymous browsing mode will not be linkable to anything the user did before.

In practice, anonymous browsing modes are not airtight. With some technical effort, an ad service that chose to do so could still track a user over time, even if the user entered anonymous browsing mode, and even if the user manually deleted cookies from his computer. There are other ways, besides cookies, for a service to detect unique marks on a user's computer; examples include so-called "Flash cookies" (which are not really cookies) as well as methods that measure unique attributes of a browser or computer. The technical details are complicated, so I will not try to explain here the limitations of these self-help measures. Suffice it to say that, given the complexity of today's web technology, there are a great many ways for an ad service to leave a subtle mark on the user's computer that can be detected later, and that it is unlikely that users will be able to shut down all of these pathways to linkability. For practical purposes we should assume that ad services will be able to link together user's activities, if they exert enough technical effort.

Once again, the fact that ad services have the technical ability to do something does not mean that responsible web services actually do it. A user who has deleted cookies or entered anonymous browsing mode has made clear his wish not to have his activities linked over time. Whether an ad service takes action to override the user's wish is a separate question. I will leave it to other witnesses to describe what their services do.

6. Allowing Users to Opt Out

Some ad services allow users to opt out of their behavioral tracking. Opt-out can mean different things for different ad services. For one ad service, opt-out may mean that the service stops consulting user profiles when choosing ads, but still continues to add information to those user profiles, and to retain the profiles for other purposes. For another ad service, opt-out may mean that the service stops gathering new information about the user, but retains and keeps using the information it already had. For a third ad service, opt-out may mean that the service discards all of the information it has about the user, and does not gather more. Users cannot tell these cases apart, unless the service makes specific statements about what opt-out means.

Designing an opt-out mechanism can be a bit tricky. On the one hand, the user has asked not to be tracked. On the other hand, the ad service must have some way to recognize when an opted-out user is visiting. A standard approach is for the ad network to put onto the user's computer a generic "opt-out" cookie, which does not uniquely identify the user's computer but simply marks the computer as one whose user has opted out from that ad service. Because cookies are visible only to the service that created them, a separate opt-out cookie is needed for each ad service from which the user wants to opt out.

Another disadvantage of using cookies as opt-out markers is that if the user takes steps to delete the cookies on his computer, or to enter anonymous browsing mode (which makes the cookies temporarily invisible), the effect will be to hide the opt-out cookie, causing the ad service to think that the user has not opted out and therefore is willing to be tracked. In this instance, deleting cookies or entering anonymous browsing mode, steps that usually protect user privacy, will have the perverse effect of removing the opt-out cookie and thereby exposing the user to greater information-gathering. The result is that cookie-based opt-out mechanisms are not as "sticky" as we might expect, and the user might have to opt out

again. In addition, because cookies are attached to a browser on an individual computer, rather than to a person, a user who opts out on one computer may still be tracked if he uses a different computer later.

Creating a single site that offers "one-stop shopping" for users who want to opt out requires cooperation among many ad services. This is what the Network Advertising Initiative (NAI), represented at this hearing by Mr. Curran, is trying to do. A user who visits the NAI site can use a single NAI page to get opt-out cookies from nearly thirty ad services.

Technical steps are possible to make opt-out more comprehensive. One approach is to modify the user's web browser software so that ad services' opt-out cookies can be permanently fixed in place, regardless of whether the user deletes other cookies or enters anonymous browsing mode. Browser extensions can be created to do this for an individual ad service's opt-out cookie, as in Google's opt-out browser extension, or for many services' opt-out cookies, as in the TACO browser extension. Alternatively, large web sites which identify their users, such as social networks or email services, could help their users get and install the full spectrum of opt-out cookies. This could be made very easy for users: the user might check a single box which would cause the social network or email site to ensure that the full spectrum of opt-out cookies remains on the user's computer, whenever the user returns to the site. Many technical options are available to help users express their opt-out preferences.

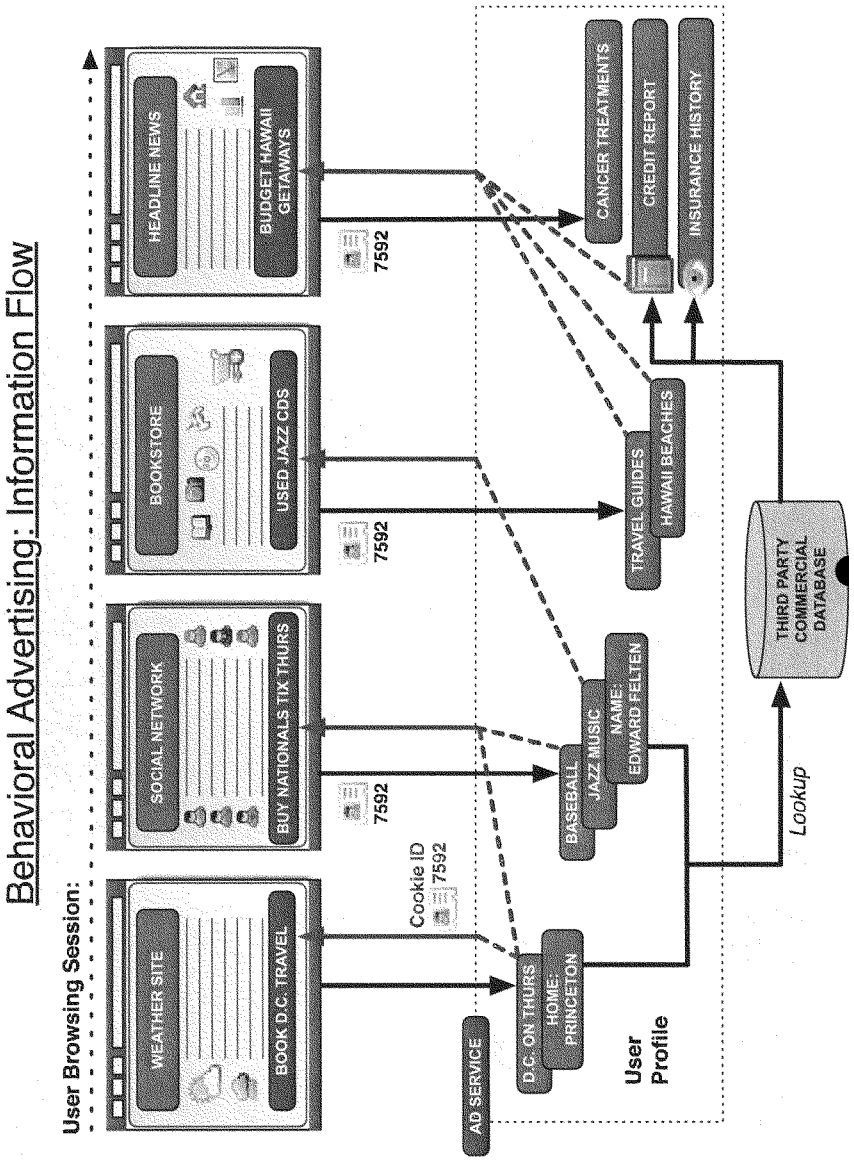
In the end, opt-out mechanisms depend on the good behavior of ad services. Users can express their desire to opt out, but there is little if anything that users can do *technically* to force ad services to respect that desire. Users can resort to the self-help mechanisms described above, but these have limited efficacy. Ultimately users must rely on well-behaved ad services to keep their promises.

7. Conclusion

Citizens are rightly concerned about the possibility that commercial entities will build extensive profiles of who they are and what they do online. Ad services are not the only parties who can assemble such profiles, but large ad services do have a prime opportunity to build profiles, due to their relationships with many content providers who can pass along information about users, and due to the ad services' ability to connect the dots by linking together a user's activities across different web sites.

All of this is possible, as a *technical* matter, which is not to say that responsible ad services do all of it, or even most of it. Ad services may be restrained by law, by self-regulation, by social norms, or by market pressures. What is clear is that technology, by itself, cannot protect users from broad gathering and use of information about what they do online.

I am grateful to both committees for holding today's important hearing. Online behavioral tracking—whether it is undertaken for advertising or for other purposes—is an important aspect of life online, for businesses and consumers alike.


Behavioral Advertising: Information Flow
User Browsing Session:
WEATHER SITE
BOOK D.C. TRAVEL
SOCIAL NETWORK
BUY NATIONALS TIX THURS
BOOKSTORE
USED JAZZ CDS
HEADLINE NEWS
BUDGET HAWAII GETAWAYS
Cookie ID
7592
7592
7592
7592
AD SERVICE
D.C. ON THURS
HOME: PRINCETON
BASEBALL
JAZZ MUSIC
NAME: EDWARD FELTEN
TRAVEL GUIDES
HAWAII BEACHES
CANCER TREATMENTS
CREDIT REPORT
INSURANCE HISTORY
User Profile
Lookup
THIRD PARTY COMMERCIAL DATABASE

Mr. RUSH. Thank you so very much. Ms. Toth, you are recognized for 5 minutes for the purpose of opening statement.

TESTIMONY OF ANNE TOTH

Ms. TOTH. Chairman Boucher and Rush, Ranking Member Stearns and Radanovich, members of the subcommittees, I appreciate the opportunity to appear before you today at this important hearing. My name is Anne Toth, and I am Yahoo!'s Vice President of Policy and Head of Privacy. I joined the company over 11 years ago and became one of the very first dedicated privacy professionals at any online company. Quite simply, my job is about making sure Yahoo! earns and maintains its users' trust each and every day. Yahoo! was founded by Jerry Yang and David Filo, who were trying to help people find information that was useful and relevant to them among the clutter of the early World Wide Web. What began as a directory of popular web sites quickly grew into a globally recognized brand that provides a wide range of innovative and useful products and services to 500 million users worldwide.

The Internet has changed a great deal, and this hearing recognizes its importance in our global economy. Gone are the days of one size fits all Internet content. Our consumers expect not only that Yahoo! will meet their needs, but that we will anticipate those needs as well. The same is true for advertising. Consumers are more likely to click on advertising that speaks directly to them and their interests. For example, Yahoo! might deliver ads featuring hybrid cars if the users spend a great deal of time on Yahoo! Green or has recently browsed car reviews on Yahoo! Autos. Put simply, customized advertising helps consumers save time and energy. As you may know, Yahoo! offers our industry leading products and services larger for free.

Our business also depends almost entirely on the trust of our users. It has been paramount to our growth and is critical for our future success. Our approach to privacy couples front end transparency, meaningful choice, and user education with back end protections for data that limit how much information and how long personal identifiers are maintained. Let us start by talking about transparency. Our leading edge privacy center, which you can see on the slide that is being projected, provides easy navigation, information on special topics, and gives prominence to our opt-out page, and actually if we could move to the next slide, making it simple for users to find and exercise their privacy choices. We have also experimented with a number of ways to provide notice and transparency outside of standard privacy policies giving users multiple privacy touch points.

We must also put control in the hands of our users. We have an opt-out that now applies to interest-based advertising both on and off the Yahoo! network of web sites. Whether a user touches us as a first party publisher or as a third party ad network, we want them to have a choice. We also didn't want users to have to redo their opt-outs again and again and took the further step of making our opt-out persistent for users who registered for a Yahoo! account. This means that these users who clear their cookies will not inadvertently clear their privacy choices at the same time. The

final aspect of the front end of privacy protection is user education. For over a year, Yahoo! has displayed on average 200 million ads per month that explain our approach to privacy. All of these front end steps are complemented by back end protections.

We focus on security and data retention as core aspects of protecting back end privacy. We recently announced the industry's leading data retention policy. Under this policy, we will retain the vast majority of our web log data in identifiable form for only 90 days. This dramatically reduces the period of time we will hold log file data in identifiable form and vastly increases the scope of data covered by the policy. The limited exceptions for this policy are explained more fully in my written testimony. We believe that our front end, back end approach to privacy builds a circle of trust with users, providing transparency, meaningful choice, and extensive education coupled with strong security and minimum data retention.

Much attention has been recently paid to the question of whether an opt-out or an opt-in approach to user control in the area of interest-based advertising is best. The answer is both. The decision about whether to ask for opt-in consent or give users the opportunity to opt out depends on the individual services being provided and the information being collected. Most advances in online privacy protection have come as a result of industry initiative and self-regulation. Market forces drive companies like Yahoo! to bring privacy innovations to customers quickly. As one company leads, many others follow or leap frog by innovating in new ways. So as Congress considers its role in helping protect consumer privacy online, Yahoo! hopes that legislators will consider an approach that enables providers to keep pace not only with technological advances but with customer demands and expectations as well.

I am very proud of Yahoo!'s record of trust and commitment to privacy, and the industry's history of responsible self-regulation. I look forward to sharing our experience with you in more depth and am happy to answer your questions. Thank you.

[The prepared statement of Ms. Toth follows:]

Testimony of Anne Toth, Vice President of Policy and Head of Privacy, Yahoo! Inc.

Before the Joint Hearing of 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 on Behavioral Advertising: Industry Practice and Consumers' Expectations.

June 18, 2009

Introduction

Chairmen Boucher and Rush, Ranking Members Stearns and Radanovich, Members of the Subcommittees, I appreciate the opportunity to appear before you today at this timely and important hearing about "Behavioral Advertising: Industry Practice and Consumers' Expectations." My name is Anne Toth and I am Yahoo!'s Vice President of Policy and Head of Privacy. I joined the company over eleven years ago and quickly became one of the first dedicated privacy professionals at an online company. In fact, I believe that I am the longest continually serving privacy officer in the history of the Internet. Quite simply, my job is about making sure Yahoo! earns and maintains our users' trust each and every day.

Yahoo! was started in a Stanford University trailer back in 1994 by Jerry Yang and David Filo who were trying to help people find information that was useful and relevant to them among the clutter of the early World Wide Web. What began as a directory of popular websites, which Jerry & David managed themselves, has since grown into a globally-recognized brand that provides a wide range of innovative and useful products and services to more than 500 million users worldwide.

It is telling that our audience has grown so large and remains so loyal after all of these years. Today, the Internet offers alternatives that are just one click away and the switching costs for web-based services are virtually zero. However, people keep coming back to Yahoo!. We believe that trust and the relationship we share with our users is what keeps those users coming back. Trust has been paramount to our growth and is critical to our future success. This is why we work so hard to reinforce that trusted relationship with our users.

The Road to Customization

Over the past few years, consumer behavior has fueled a tremendous amount of innovation in the kinds of products and services that are available on the Internet. Today users expect their content and services to be personally relevant, and they are seeking greater control over what they want, when they want it, and how it's delivered. Gone are the days of one-size-fits-all. Customization is the new game in town. In fact, there is a growing expectation from consumers that Yahoo! will not simply *meet* their needs but will *anticipate* those needs based on a combination of customization and the trusted relationship we have with them.

Just as our users value the personally relevant content we provide, we take a similar approach in the way we deliver advertising. Not surprisingly, consumers are more likely to "click" on advertising that speaks directly to them and their interests. For example, Yahoo! might deliver ads about travel deals if a user has recently researched vacation destinations for their summer family getaway, or ads featuring hybrid cars if a user has spent a great deal of time on Yahoo! Green or has recently browsed car reviews on Yahoo! Autos. Put simply, customized advertising helps consumers save time and energy since they are more likely to find what they are looking for when we've anticipated what they are most interested in.

The customized ads on our pages are intended to enhance our users' experience, and revenues from those ads have allowed Yahoo! and many other sites on the Internet to offer content and services that are largely free to consumers. There is an important value exchange here. Customized advertising works because users enjoy a more relevant and useful experience, advertisers are better able to reach their desired audience, and web publishers are better able to support free content and services. This model is the foundation of a vibrant ecosystem that has helped this industry flourish. Indeed, we believe that during difficult economic times, enabling consumers to access the content and services they desire for free in an advertiser-supported fashion represents an important consumer benefit.

Yahoo!'s Commitment to Trust and Leadership on Privacy: A Front- and Back-End Approach

As we have said before, our business depends almost entirely on the trust of our users. At Yahoo! we have developed an approach to privacy that couples front-end transparency, meaningful choice, and user education with back-end protections for data that limit how much information and how long personal identifiers are maintained.

Let's start by talking about transparency. Yahoo! recognized very early that our users should understand what information we collect, how we collect it and how it is used, and just as importantly – how we manage and protect it. In 1998, we became one of the very first companies in the United States to develop and publish a comprehensive privacy policy, which could be found through a prominent link on our home page. In 2002, Yahoo! again led the industry by introducing a layered "Privacy Center" model on top of our existing privacy policy. This model was the result of our rapid expansion into a wide array of online services, and it

helped users readily find privacy-related information about the specific Yahoo! services they used – without requiring them to wade through information about services they did not. In 2008, we redesigned our Privacy Center to further improve navigation, provide more information on special topics, and to give special prominence to our opt-out page so users could easily find and exercise their choice to decline interest-based advertising.

Today, Yahoo! provides ready access to our privacy policy on virtually all of the pages across our family of web sites. In addition, Yahoo! has experimented with a number of ways to provide notice and transparency *outside* of standard privacy policies. For instance, Yahoo! is proud to have partnered with eBay on their AdChoice model in 2007, which explains interest-based advertising to users at the time when an ad is delivered. Through the AdChoice pages, users can learn more about customized advertising and the choices they have, as well as access Yahoo!'s opt-out. In addition to our collaboration with eBay, Yahoo! has worked with other privacy-minded partners on alternate types of enhanced privacy notices. We are also working with members of the Network Advertising Initiative and the Interactive Advertising Bureau to explore new technological means to deliver privacy notices to consumers within the context of the advertising experience itself.

Providing users with easy access to privacy policies and giving them choice is the first step toward building and maintaining a trusted relationship. The second is to have policies that put meaningful control in the hands of users. Yahoo! has worked continually over the last several years to improve our interest-based advertising opt-out. Last summer, we announced that our opt-out would apply to interest-based advertising both *on and off* of the Yahoo! network of web sites – in other words, whether we touch users as a first-party publisher or as a third-party ad

network, we want users to have a choice. Before that time we had offered an opt-out that was consistent with the NAI's self-regulatory principles that require an opt-out when serving interest-based ads in a "third-party" capacity.

While we believe that interest-based advertising provides the most compelling experience for our users, we also know that there are some users who would rather not see those kinds of ads. When we expanded our opt-out, we made the assumption that users who don't want to get interest-based ads off of Yahoo! sites probably wouldn't want to see them anywhere the Yahoo! Ad Network serves advertising. While this change went above and beyond the industry practice, it further demonstrates the lengths we are willing to go to in maintaining trust with our users.

In the interest of providing a positive consumer experience, we also assumed that consumers who chose to opt out once generally didn't want to do so again and again. Yahoo! addressed this issue by making our opt-out persistent for users who have registered for a Yahoo! account. The growing use of browser tools by users to clear cookies – the files that web sites use to provide customized services to users – has on occasion inadvertently weakened users' opt-out choices. We were concerned that users would have to set their Yahoo! opt-out every time they clear their browser cookies or use a different Internet browser. Now, these users simply have to log into their accounts and Yahoo! is able to refresh these use their opt-outs on that browser, also making these users' opt-outs easily portable. When an opted-out user logs in from home or from work, Yahoo! automatically copies over their opt-out on every computer they use, so that they don't have to download a plug-in for every browser and every device they might use to access the Internet.

Of course, our privacy protection is only effective if our users know about it. Therefore, the final aspect of the "front end" of privacy protection is user education. We want to ensure that even those users who do not seek out privacy policies understand the services we offer and the options they have. Beginning last spring, we ran an extensive user education campaign that explained Yahoo!'s approach to privacy, our customization services, as well as the tools we provide such as our opt-out. Over the course of the last year, these ads were shown on average over 200 million times per month and they are still running today. Research has shown that users are becoming more accustomed to "targeted advertising" and more aware of it. In a recent survey 72 percent of participants said they preferred to be served targeted advertisements from brands they know and trust over irrelevant, intrusive advertisements.[1] Technology can be intimidating for some, so we think that being transparent about privacy benefits all users.

All of our front-end steps – transparency, meaningful choice, and user education – are complemented by back-end protections as well. We focus on security as well as data retention as core aspects of protecting back-end privacy. We work continuously to protect user information with a dedicated team of engineers for whom security is top-of-mind. We assist all of our developers so that they build security into our products and services. In addition, we are also proud to have recently announced the industry's leading data retention policy – one that is more privacy-protective than our competitors' policies both in terms of scope of data covered and in terms of time the web log data is held in identifiable form. Even if a user takes no steps to engage with our notices or elects not to opt out on the front end, we still protect and manage personal data in a privacy-enhancing way on the back end.

[1] TRUSTe-TNS 2009 Consumer Attitudes About Behavioral Targeting
http://www.truste.com/about/bt_overview.php

We announced our new data retention policy at the end of 2008, after a comprehensive year-long review of our data tools and systems. Under the new policy we will retain the vast majority of our web log data in identifiable form for only 90 days.[2] This new policy is notable because it dramatically reduces the period of time we will hold log file data in identifiable form while also vastly increasing the scope of data covered by the policy. It replaces our prior 13-month data retention commitment which covered search log data only, and expands the policy beyond search to include identifiable data associated with ad views, ad clicks, page views and page clicks – the very data informing our ad systems. There are limited exceptions to this policy – for instance, Yahoo! will retain data used to help prevent fraud and preserve security for up to six months – but only for that purpose – and we will retain data needed to meet legal obligations. These narrow exceptions enable us to de-identify more data far sooner than we did previously.

We have also made smaller incremental improvements. For example, when we made our data retention policy announcement, our intention was to de-identify IP addresses by deleting only the final "octet" or last set of numbers from the IP addresses. However, we recently decided that it would simplify our process to delete the entire IP address within that 90-day period.

We believe that our front-end/back-end approach to privacy is not just comprehensive but industry leading. Through it we build a circle of trust with our users – providing transparency,

---

[2] Yahoo! announced its log file data retention policy in December 2008. Under this policy web log data such as page views, page clicks, ad views, ad clicks and search queries will be de-identified within 90 days. Exceptions to this policy include web log data that is used to help detect and defend against fraudulent activity and preserve system security, which may be held in identifiable form for up to 6 months, but is onlyl used for that purpose. We may also retain web log data in identifiable form for longer periods in order to meet legal obligations. Yahoo! expects its web log data retention policy to be fully implemented on a global basis by mid-year 2010.

meaningful choice and extensive education coupled with strong security and minimum data retention.

Privacy Defaults Are Important: Opt In or Opt Out?

Much attention has been paid recently to the question of whether an opt-out or an opt-in approach to user control in the area of interest-based Internet advertising is best. The answer is that it's not one or the other – it's both. Some services and models should require an opt-in approach, while, for other models, an opt-out is a more appropriate default. Yahoo! requires opt-in consent in some situations today outside the advertising context that inform our thinking on this topic. If Yahoo! hosts a promotion for an advertising partner where an online form with personally identifiable information is filled out by the user, we require users to affirmatively consent to sending their information to the partner prior to submitting the form. We also have a downloadable Yahoo! toolbar product that allows users to opt in to a research panel where their browser's clickstream data is collected by Yahoo! for research and product improvement purposes. Because this feature allows Yahoo! to see every page visited by a user across the Internet, users must opt in to activate it. Ultimately, the decision about whether to ask for opt-in consent or give users the opportunity to opt-out depends on the individual services being provided.

As the person leading a team of people charged with thinking about privacy at Yahoo! every day, I know that there is no one-size-fits-all approach to privacy. When determining whether to implement an opt-in or opt-out for a particular service it is necessary for companies to consider whether everything a user does online is collected through that service. This is especially true if this online information is connected to a users' name and address. But for most

online advertising, a good opt-out paired with transparency and responsible data retention policies is the right default setting for users. A good opt-out needs to be prominent, readily accessible, clearly conveyed, and give users options to make it persistent. Furthermore, responsible data retention minimizes the amount of time data is held in identifiable form in order to provide quality services, billing, fraud protection, and to meet legal obligations.

Most advances in online privacy protection have come as a result of industry initiative and self-regulation. Market forces drive companies like Yahoo! to bring privacy innovations to our customers quickly. As one company leads, many others follow or leapfrog by innovating in other ways. Self-regulation then raises the bar to bring the rest of industry along with commitments in the areas of notice, choice, security, and enforcement. One of the reasons self-regulatory initiatives have been successful in the online environment over the last decade is that companies have responded quickly as markets evolved, services became more and more sophisticated and interfaces changed. As Congress considers its role in helping protect consumer privacy online, Yahoo! hopes that legislators will consider an approach that enables providers to keep pace not only with technological advances but with consumer demands and expectations as well.

Conclusion

At Yahoo! we are building products and services for hundreds of millions of users, and with that comes awesome responsibilities. It's not enough to simply build great products – although we are very proud of our accomplishments. What makes it all worthwhile is the longstanding relationship we share with our users. We take that responsibility very seriously and work to enhance that trusted relationship each and every day. Congress also has an important

role to play in making sure that consumers are protected as they seek out new customized products and services online. Yahoo! looks forward to working with you as you explore ways to do just that.

Mr. RUSH. Thank you, Ms. Toth. Now the chair recognizes Ms. Wong. Ms. Wong, you have 5 minutes or thereabouts.

TESTIMONY OF NICOLE WONG

Ms. WONG. Chairmen Rush and Boucher, Ranking Members Radanovich and Stearns, and members of the committee, I am pleased to appear before you this evening to discuss online advertising and the ways that Google protects our users' privacy. Online advertising is critically important to our economy. It promotes freer, more robust and more diverse speech, and enables many thousands of small businesses to connect with consumers across the nation and around the world. It helps support the hundreds of thousands of blogs, online newspapers, and other web publications that we read every day. Over the last decade, the industry had struggled with the challenges of providing behavioral advertising. On the one hand, well-tailored ads benefit consumers, advertisers, and publishers alike. On the other hand, we recognize the need to deliver relevant ads while respecting users' privacy.

In March, Google entered the space and announced our release of interest-based advertising for our AdSense partner sites and for YouTube. Interest-based advertising uses information about the web pages people visit to make the online ads they see more relevant and relevant advertising has fueled much of the content, products, and services available on the Internet today. As Google prepared to rule out interest-based advertising, we talked to many users, privacy and consumer advocates and government experts. Those conversations led us to realize that we needed to solve 3 important issues in order to provide consumers with greater transparency and choice, which are core design principles at Google.

First, who served the ad? Second, what information is being collected and how is it being used? And, finally, how can consumers be given more control over how their information is used? This evening I would like to show you how we answered each of those questions with the launch of interest-based advertising, which includes innovative, consumer-friendly features to provide meaningful transparency and choice for our users. When you see an online ad today you generally don't know much about that ad. It is difficult to tell who provided the ad and how your information is being collected and used. Google is trying to solve this problem by providing a link to more information right in the ad, as you can see, where it is labeled Ads By Google. This is very different from current industry practices, but we believe that it is important to provide users with more information about the ad right at the point of interaction.

We believe that this is a significant innovation that empowers consumers and we think that this is the direction that many in the industry are going. If you are curious about getting information about the ad, you can click on the Google link and navigate to an information page about Google ads, which you can see here. On this page, you are invited to visit our ads preference manager, which helps explain in plain language user friendly format what information is being collected, how it is being used, and how you can exercise choice and get more information about how this advertising product works. Here is the ads preference manager. This in-

novative tool allows you to see what interests are associated with an advertising cookie, the double click cookie, that is set in the browser you are using.

In this case, Google has inferred that my cookie should be associated with hybrid cars, movie rentals and sales, and real estate. This is because I visited sites using the browser about hybrids, movies, and real estate. Before Google introduced the ads preference manager, most users had no idea what interests were being associated with their cookies online by advertising companies. We are the first major company to introduce this kind of transparency. Now you can see those interests, and if you don't agree with those interests, maybe you are not a movie fan or you simply don't want to see ads about movies, you can delete any one of them or a few or as many as you want. So, for example, if you want to delete movie rentals and sales, you can do that with one click, and I have just done that.

Likewise, you can add any interests you like. Note that Google does not use sensitive categories so there is nothing in here about sexual orientation, religious affiliation, health status or the like, but there are many, many other options. For example, if you are a sports fan you can associate your cookie with sports, and with a click I have decided that I would like to receive ads personalized for sports fans. If you prefer not to see interest-based ads from Google, you can opt out at any time with one click. After you opt out, Google won't collect information for interest-based advertising and you won't receive interest-based ads from us. You will still see ads, but they may not be as relevant. The opt-out is achieved by attaching an opt out cookie to your browser. Opt out cookies in the industry, however, have traditionally not been persistent. That is, they are often inadvertently deleted from the browser when a user deletes her cookies.

So our engineers have developed a tool that was not previously available that makes Google's opt out cookie permanent even when users clear other cookies from their browsers. After you opt out, just click the download button and follow the instructions to install a browser plug-in that saves your opt out settings even when you clear your cookies. I hope this gives you a better idea how Google shows interest-based ads and how we provide users with transparency in the right place at the right time, as well as meaningful, granular, and user-friendly traces for setting ad preferences or opting out. Thank you very much for your time.

[The prepared statement of Ms. Wong follows:]

Google™

Testimony of Nicole Wong
Deputy General Counsel, Google Inc.
House Committee on Energy and Commerce
Subcommittee on Communications, Technology, and the Internet and
Subcommittee on Commerce, Trade, and Consumer Protection
Hearing on the potential privacy implications of behavioral advertising
June 18, 2009

Chairman Boucher, Chairman Rush, Ranking Member Stearns, Ranking Member Radanovich, and members of the Committee.

I'm pleased to appear before you this morning to discuss online advertising and the ways that Google protects our users' privacy. My name is Nicole Wong, and I am Google's Deputy General Counsel responsible for privacy. In this role, I work with our product teams and other privacy professionals at Google to ensure compliance with privacy laws and develop best practices for protecting our users' privacy.

Online advertising is relatively young and a very small piece of the advertising market as a whole. It accounts for approximately nine percent of all advertising revenue, and Google represents only 30 percent of online advertising revenue, according to Cowen and Company, in a business environment characterized by strong competition, significant innovation, and signs of continuing growth despite a challenging economic climate.

At Google we believe that our online advertising business has succeeded because our most important advertising goal is to deliver ads that benefit our users. From its inception, Google has focused on providing the best user experience possible. We do this, for example, by ensuring that advertising on our site delivers relevant content that is not a distraction. In fact, we endeavor to make ads that appear next to search results just as useful to Google's users as the search results themselves.

Putting our users first also means that we are deeply committed to their privacy, and our products and policies demonstrate that commitment. We believe that success in online advertising and protecting our users' privacy are not mutually exclusive goals. We work hard to provide advertising that is transparent to users, provides them with appropriate choices, and protects any personal information that we collect from inappropriate access by third parties. In fact, we design all of our products according to the three design principles of transparency, choice, and security.

In my written testimony, I would like to cover three key points:

- First, I'll describe Google's main advertising products and the significant benefits that we at Google believe online advertising brings to advertisers, online publishers, and individual Internet users.

- Second, I'll discuss Google's approach to privacy, specific steps that we take to protect our users' privacy, and our recent release of a new advertising product that we call interest-based advertising.

- And finally, I'll explore ideas and make recommendations for how to better protect Internet users' privacy with respect to advertising as well as more generally as increasing amounts of information move to the Internet.

The Benefits of Online Advertising

Google offers three main advertising products: AdWords, AdSense for Search, and AdSense for Content. AdWords is an advertiser-facing product that lets advertisers run ads on Google and on third-party sites that partner with us as part of the Google Content Network. AdSense for Search is a publisher-facing product that shows ads in response to search queries entered by users of our partners' search engines, including AOL and Ask.com. AdSense for Content is a publisher-facing product that shows ads to people who visit our Google Content Network partners' websites, based on the content of the page being viewed by a user. The vast majority of Google's revenue comes from these products.

In addition to AdWords and AdSense, our DoubleClick business lets advertisers and publishers take advantage of our efficient ad serving and reporting infrastructure.

In March of this year, we launched a new offering for AdSense for Content called interest-based advertising, which enables ads that are based on users' interests rather than the content of the page that they are viewing. I discuss interest-based advertising at length later in my testimony.

Advertisers, online publishers, and consumers all benefit from our advertising services. I'll start with consumers – our users – on whom our business depends.

In our experience, users value the advertisements that we deliver along with search results and other web content because the ads help connect them to the information, products, and services they're looking for. For example, the ads we deliver to our users complement the natural search results that we provide because our users are often searching for products and services that our advertisers offer. Making this connection is critical, and we strive to deliver the ads that are the most relevant to our users, not just the ones that generate the most revenue for us. We do this through our innovative ad auction system, which evaluates the relevance or usefulness of an ad to our users based on their search queries or the content that they are viewing. And in our pay-per-click pricing model, we generate revenue only when a user is interested enough to click on an ad.

Online advertising makes it possible for Google to offer dozens of free products to our users – everything from search and email to our word processing application Google Docs. Each of these products reflects our commitment to improving our users' online experience. For example, Google Docs allows multiple users to collaborate on a single document, presentation, or spreadsheet at the same time. And all of our products – including YouTube, Google Earth, and Gmail – are free to individuals for personal use. Current and future prospects for online advertising support the creation, development, and ongoing work on these and future products.

And our ads aren't always commercial. We run a program called Google Grants that provides free advertising to not-for-profit organizations supporting science and technology, education, global public health, the environment, youth advocacy, and the arts. For example the Dungannon Development Commission, which helps families in Dungannon, Virginia with housing, family services, and food drives, has seen a 50 percent increase in visits to its website (located at www.ddcinc.org) over the 18 months it's been associated with Google Grants. And Chicago-based Project Exploration, which makes science accessible to the public – especially minority youth and girls – through personalized experiences with scientists and science, has used Google Grants to generate more than 40 percent of the Internet traffic

going to www.projectexploration.org. Since April 2003, our grantees have collectively received over $440 million in free advertising.

Our advertising network also helps small businesses connect with consumers that they otherwise would not reach, and do so affordably, efficiently, and effectively. The advertiser decides the maximum amount of money it wishes to spend on advertising and, as noted above, in the cost-per-click payment model the advertiser pays Google only when a user actually clicks on an ad.

Here are just some examples of small businesses and not-for-profit organizations that are using AdWords:

- Military spouse Meredith Levya of Schertz, Texas, founded eCarePackage.org after the attacks of September 11, 2001 to support our service members and their families with care packages, toiletries, snacks, and other necessities. Ms. Levya relies solely on AdWords to market nationally and significantly boost eCarePackage's ability to find people who want to show support to the troops.

- SmallConcept.com uses AdWords to drive customers to their store located in north Atlanta, Georgia, as well as to their online store. The family-owned business estimates that AdWords generates $10,000 worth of sales each month.

- Jason Pelletier and Jessica Jensen of Los Angeles, California, created LowImpactLiving.com to educate on the benefits of green living and advise on how to lower your environmental impact. They use AdWords to reach out to environmentally conscious consumers and also monetize their site to deliver relevant AdWords ads alongside their content.

- Zingerman's Deli (www.zingermansdeli.com) of Ann Arbor, Michigan, has been using AdWords since the holiday season of 2007 when they saw an immediate 375 percent return on investment from advertising with Google.

Online advertising also promotes freer, more robust, and more diverse speech. This advertising supports the explosive growth of new online newspapers, blogs, and other online publications we have seen in the last few years. Our AdSense product lets publishers generate revenue from ads that we place on their websites, increasing the size and capabilities of the teams working on online publications. We know that many small website owners can afford to dedicate themselves to their sites full-time because of online advertising.

AdSense revenues support hundreds of thousands of diverse websites, and a significant percentage of the revenue we earn from advertising ends up in the hands of the bloggers and website operators who partner with us by featuring ads provided by Google. For example, last year we paid over $5 billion in advertising revenue from our AdSense program to our publishing partners.

The vast majority of these AdSense partners are small businesses. For example, brothers Maxwell and Oliver Ryan leveraged AdSense to generate revenue for their home interior design resources site ApartmentTherapy.com. The New York City business soon expanded to branches in Boston, Chicago, Los Angeles, San Francisco, and Washington, DC in part by leveraging AdSense's ability to deliver relevant local advertisements. And in Alpharetta, Georgia, Stephanie and Rick Jaworski launched JoyofBaking.com as an outlet for Stephanie's passion in baking. The couple placed Google Ads on the site to earn revenue, and have now built a wildly successful business that sees over a million page views a month, which spikes

significantly during the holidays. Similar small business success stories are happening all across the United States.

AdSense partners also include hundreds of major newspapers across the country, like USA Today (www.usatoday.com), the Washington Post (www.washingtonpost.com), and the Los Angeles Times (www.latimes.com), as well as hundreds of smaller online news sites. We also work with online newspapers by sending them over one billion visits per month from our search engine and from Google News, our specialized service designed specifically for users who are looking for news articles.

It's no mistake that I've focused mainly on individual users, small publishers, and small advertisers. Google's business model has extended to what's known as the "long tail" of the Internet – the millions of individuals and small businesses that cater to and need to connect with niche interests and markets. Google's advertising programs lower the barrier to entry for small publishers and advertisers alike, and connect them with users who are interested in what they have to say or sell. As our advertising business continues to grow and evolve, we will continue working hard to encourage the development of the long tail.

Google's Focus on Privacy

We believe user trust is essential to building the best possible products. With every Google product, we work hard to earn and keep that trust with a long-standing commitment to protect the privacy of our users' personal information. We make privacy a priority because our business depends on it. If our users are uncomfortable with Google's approach to privacy, they are only one click away from switching to a competitor's services. As a result, for example, we are not in the business of selling our users' personal information.

Because user trust is so critical to us, we've ensured that privacy considerations are deeply embedded in our culture. Though I am Google's Deputy General Counsel responsible for privacy, I am just one of many individuals at Google who work on privacy, including global privacy attorneys and other Google employees who work on privacy technology, policy, and compliance initiatives. For example, our team of product counsels works with engineers and product managers from the beginning of product development to ensure that our products protect our users' privacy. We also have product managers dedicated to privacy and other trust and safety issues. And our Privacy Council, a cross-functional group of Google employees, helps us identify and address potential privacy issues.

Google's focus on user trust and privacy means that our product teams are thinking about user privacy by building privacy protections into our products from the ground up. For example, we have designed most of our products to allow people to use them without registering, and to avoid any use of personally identifiable data unless that use is fully disclosed in our privacy policy.

We have also made sure that three design fundamentals – all of them rooted in fair information principles – are at the bedrock of our privacy products and practices:

- **Transparency**: We believe in being upfront with our users about what information we collect and how we use it so that they can make informed choices about their personal information. We have been an industry leader in finding new ways to make our privacy practices more transparently to our users. Our Google Privacy Channel on YouTube (found at www.youtube.com/googleprivacy) features privacy videos that explain our privacy policies, practices, and product features in simple, plain language, and through our Privacy Center (found at www.google.com/privacy).

- **Choice:** We strive to design our products in a way that gives users meaningful choices about how they use our services and what information they provide to us. Many of our products, including our Search service, do not require users to provide any personally identifying information at all. When we do ask for personal information, we provide features that give users control over that information. For example, our Google Talk instant messaging service includes an "off the record" feature that prevents either party from storing the chat. In addition, we provide choice through our Data Liberation team, which is focused on making sure that our users control their data and can export it from our products and services conveniently and without expense. This effort ensures both a great user experience and strong competition on the web. Not trapping our users' data is critical to ensuring that they have choice and control over their information.

- **Security:** Because we take security very seriously, we have some of the best engineers in the world working at Google to secure information. Much of their work is confidential, but we do want to highlight three ways we're protecting our users' data. First, our security philosophy is one of layered protection. The best analogy to this philosophy is how you secure your home. You put private information in a safe, you secure the safe in your house, you have locks and an alarm system for the house, and finally you have a neighborhood watch program or the police monitoring your neighborhood. Second, these layers of protection are built on what we believe is the best security technology in the world, including both products developed by others and our own security technology. We're also constantly seeking more ways to use encryption and other technical measures to protect data, while still maintaining a great user experience. Finally, in addition to technology, we have processes in place that dictate how we secure confidential information at Google, and we limit access to sensitive information to a very limited number of Googlers, and then only when there is good reason to access the information. More information about our approach to security can be found on the Official Google Blog located at googleblog.blogspot.com/2008/03/how-google-keeps-your-information.html.

Interest-Based Advertising

In March of this year, Google announced our beta release of interest-based advertising – IBA – for our AdSense partner sites and YouTube. IBA uses information about the web pages people visit and YouTube videos watched to make the online ads they see more relevant. In addition, IBA allows advertisers to serve subsequent ads to users after they have left the advertiser's website. For example, if a user visits a website that sells pet supplies, she might see an ad for cat food the next time she browses other sites that display interest-based ads from Google.

Providing such advertising has proven to be a challenging policy issue for advertisers, publishers, Internet advertising companies, and regulators over the last decade. On the one hand, well-tailored ads benefit consumers, advertisers, and publishers alike. On the other hand, the industry has long struggled with how to deliver this kind of relevant advertising in a way that respects users' privacy.

In February, the Federal Trade Commission released its principles for online advertising (www2.ftc.gov/os/2009/02/P085400behavadreport.pdf). Likewise, non-governmental organizations interested in consumer protection and privacy also recently issued guidelines. The Network Advertising Initiative released its 2008 Self-Regulatory Code of Conduct in December of last year (www.networkadvertising.org/networks/2008%20NAI%20Principles_final%20for%20Website.pdf), and the Center for Democracy and Technology released its Threshold Analysis for Online Advertising Practices in January of this year (www.cdt.org/privacy/20090128threshold.pdf). There is a consistent message in all of these guidelines: consumers need and deserve greater transparency and choice when it

comes to online advertising, and in particular third-party advertising.

As Google prepared to roll out interest-based advertising, we consulted with many users, privacy and consumer advocates, and government experts. By listening to them and by relying on the creativity of our engineers, we built a product that goes beyond existing self-regulatory and industry standards. We are pleased that our launch of IBA includes innovative and consumer-friendly features that provide meaningful transparency and choice for our users.

Transparency in the right place and at the right time. When users see online ads today, they often don't know what information is being collected, who provided the ad, and sometimes who the advertiser is. We already clearly label most of the ads provided by Google on the AdSense partner network and on YouTube. The vast majority of Google Content Network ads contain in-ad notice, letting users with one click get more information about how we serve ads, and the information we use to show ads. This year we will expand the range of ad formats and publishers that display links that provide a way to learn more and make choices about Google's ad serving.

Meaningful, granular, and user-friendly choice. For the first time, people have a say in the types of ads they see by using our new Ads Preferences Manager (www.google.com/ads/preferences/). With this tool, users can view, add and remove the categories that are used to show them interest-based ads (sports, travel, cooking, etc.) when they visit one of our AdSense partners' websites or YouTube. To provide greater privacy protections to users, we will not serve interest-based ads based on sensitive interest categories. For example, we don't have health status interest categories or interest categories for children.

Tools that respect users' choices. Users can opt out of interest-based ads altogether, although it means they will probably see advertising that's less relevant and useful on our partners' websites or YouTube. The opt-out is achieved by attaching an "opt-out cookie" – a small file containing a string of characters that stores a preference for opting out – to a user's browser. More specifically, when a user opts out, an opt-out cookie that has the text "OPTOUT" where a unique ID would otherwise be is attached to the user's browser. If a user views the opt-out cookie, she will literally see the text "OPTOUT". This means that there is no further cookie-based information collected about that user (specific to the browser and computer that they are on). Opt-out cookies in the industry, however, have traditionally not been permanent. So Google's engineers also developed tools to make our opt-out cookie permanent, even when users clear other cookies from their browsers (see www.google.com/ads/preferences/plugin/).

Transparency beyond privacy policies. With interest-based advertising, we're continuing to explore new ways of communicating with our users on privacy. We've revamped the advertising section of our Privacy Center. And the Ads Preferences Manager features a video that explains in plain language how interest-based advertising works. All of the videos on the Google Privacy Channel on YouTube (www.youtube.com/googleprivacy) are open for comment and we look forward to hearing feedback from our users.

We've built our business by earning and keeping the trust of our users. And we'll continue our dialogue with them and with other stakeholders as we develop new products to make the ads we show our users more relevant and useful.

<u>Continuing Efforts to Better Protect Consumer Privacy</u>

In our quickly evolving business environment, ensuring that we earn and keep our users' trust is an essential constant for building the best possible products. With every Google product, we work hard to earn and keep that trust with a long-standing commitment to protect the privacy of our users' personal

information. As stated above, the bedrock of our privacy practices are three design fundamentals: transparency, choice, and security.

We have also found that innovation is a critical part of our approach to privacy. To best innovate in privacy, we welcome the feedback of privacy advocates, government experts, our users, and other stakeholders. This feedback, and our own internal discussions about how to protect privacy, has led us to several privacy innovations, including our development of new privacy tools for new products and our decision last year to anonymize our server logs after nine months for IP addresses and 18 months for cookies.

In the spirit of encouraging continuing innovation that enhances consumer privacy, we offer the following policy and technology recommendations – some of which can be accomplished by the private sector and some of which involve a government role.

Our ideas and recommendations endorse a baseline and robust level of privacy protections for everyone. On that foundation we believe that the private sector and government should cooperate to educate and inform consumers about privacy issues and to establish best practices that will help guide the development of the quickly evolving and innovative online advertising space. In addition, we believe that Congress should continue exploring online advertising practices with a particular focus on industry practices that may not be transparent. Finally, we believe that Google and others in the online advertising industry should work to provide tools to better protect individuals' privacy, and that government should encourage companies to experiment with new and innovative ways of protecting consumers' privacy.

Comprehensive Federal Privacy Legislation

Google supports the passage of a comprehensive federal privacy law that would accomplish several goals: building consumer trust and protections, establishing a uniform online and offline framework for privacy, creating expectations of privacy from one jurisdiction to another, and putting penalties in place to punish and deter bad actors. We believe that as information flows increase and more and more information is processed and stored – on remote servers rather than on users' or businesses' own computers – there is a greater need for uniform data safeguards, data breach notification procedures, and stronger procedural protections covering government and third-party litigant access to individuals' information.

Behavioral Advertising Principles and Self-Regulation

We participated actively in the Federal Trade Commission's efforts to develop privacy principles relating to online privacy and behavioral advertising, and we applaud the Commission's efforts to move industry towards stronger and broader self-regulation in the behavioral advertising space.

Google is a member of the Network Advertising Initiative (NAI), a self-regulatory organization chartered in 2000 to establish privacy principles for emerging online behavioral advertising technologies. In response to the FTC's call for stronger and broader self-regulation, the NAI is currently working with its members to undertake several new initiatives relating to notice in or around display advertisements and persistent opt-out technology. These efforts are very much in line with Google's own in-ad notice and persistent opt-out plugin tool.

Also in response to the Commission's call for a broad and strong self-regulatory system, Google has been working for several months with numerous leading companies and associations on cross-industry self-regulatory principles designed to provide consumers with greater transparency and choice regarding the online advertising they see. The effort was initiated by some of the nation's largest and most prominent

national advertising and marketing and publisher trade associations including the Association of National Advertisers, the American Association of Advertising Agencies, the Direct Marketing Association, and the Interactive Advertising Bureau. Though it has not been finalized, we are hopeful that this self-regulation effort will result in a benefit to American consumers through greater transparency and choice in online behavioral advertising.

We trust that this Committee will welcome these industry efforts at stronger and broader self-regulation as a positive initiative that will benefit consumers. At the same time, in the interest of consumers, we hope that the Committee will encourage industry to adhere to these standards and always be on the lookout for areas of improvement.

Empowering Consumers through Education and Transparency

Transparency is one of Google's bedrock design principles because we believe that informed and knowledgeable users are best able to protect their privacy. We believe that both the private sector and the government, including agencies like the FTC, can and should provide more information about what kinds of personal information are collected by companies, how such data is used, and what steps consumers can take to better protect their privacy.

At Google, for example, we take great pride in our effort to provide our users with a better understanding of how we collect, use, and protect their data through a series of short videos available at Google.com and on YouTube, as well as through blog posts. Too often, companies view their online privacy policy – which is often impenetrable to the average user – as the beginning and end of their privacy obligations. Companies that interact with consumers need to do more than simply provide and link to privacy policies; all we need to offer consumer-friendly materials in different media to help users better understand how their information is collected and used, and what choices they have to protect their privacy.

We also believe in "transparency in context" so that consumers can benefit from privacy information when and where they're actually using a product or service, in addition to through a privacy policy. The concept of transparency in context underlies our desire to provide in-ad notice for interest-based ads. With such notice, consumers have easy access to both information and choice tools at the point of interaction with the relevant product.

Continuing Development of Technology to Empower Users

Products like Google Toolbar let a user choose to not have data collected, and that choice persists even if all cookies are cleared and until the user chooses to have data collected. Similarly, as described above, our interest-based advertising product allows users to opt out of collection and use of data for that type of advertising until they make an affirmative choice to opt back into IBA.

Google also offers features like Web History, which allows users to view and search all search queries they have made on Google Search while logged into Google. Web History also lets users delete and thus disassociate from their account information any searches that they conduct while they are logged in. Users can also pause Web History altogether if they do not want their searches to be associated with their account information – and this choice persists until users choose to resume Web History.

Like Google, many other Internet companies that are consumer-facing and have strong trust relationships with consumers have developed tools that empower consumers. We applaud their efforts, and we believe that industry can and should continue to ensure both the availability of more transparency and greater user choices that persist at the user's option. Google looks forward to continuing to release products with

features and tools that uphold our commitment to providing users with greater transparency and more choice and control.

Further Exploration of Industry Practices

We believe that online advertising is critical to the success of the Internet and of the economy more broadly. In fact, a study commissioned by the Interactive Advertising Bureau and released last week put some real numbers on this very point. According to Harvard Business School professors John Deighton and John Quelch, the Internet is responsible for 3.1 million American jobs and $300 billion in economic activity spread throughout the United States. As Professors Deighton and Quelch put it, the web "has created unprecedented opportunities for growth among small businesses and individual entrepreneurs."

Of course, the online advertising industry, like all industries, has the obligation to engage in responsible business practices, and ought to be transparent with Congress about those practices. Already, the Network Advertising Initiative – of which Google is a member – places limitations on its members' activities. For example, the NAI requires opt-in consent from consumers when their personally identifiable information (PII) is merged with previously collected non-PII, as well as when advertisers use sensitive consumer information for behavioral advertising.

There may also be industry practices that are not transparent and may not be in consumers' best interests that require exploration by this Committee and Congress generally. In addition, the Committee should take a holistic approach to this issue, especially given ongoing efforts to bring together online and offline data, thus blurring the lines between the two worlds. The real potential misuse of personal information (such as the sale of personal information without an individual's consent), and not simply the platform on which it is gathered, should be at the core of further Committee action.

Conclusion

Chairman Boucher, Chairman Rush, Ranking Member Stearns, Ranking Member Radanovich, and members of the Committee, thank you for inviting me to testify today. We at Google appreciate the opportunity to demonstrate both the benefits of online advertising and how our company has helped lead in the effort to protect consumers' privacy by providing them with transparency, choice, and security.

I look forward to answering any questions you might have about our efforts, and Google looks forward to working with members of the Committee and others in the development of better privacy protections.

Thank you.

Mr. RUSH. Next, we welcome Mr. Kelly. Mr. Kelly, you are recognized for 5 minutes.

TESTIMONY OF CHRISTOPHER M. KELLY

Mr. KELLY. Thank you very much. Chairman Rush and Boucher, and Ranking Members Radanovich and Stearns, and members of the subcommittees, thank you for this opportunity to address important privacy matters on the Internet. We agree with you that protecting privacy is critical to the future growth of the Internet economy. Facebook now serves more than 200 million active users worldwide, roughly 70 million of whom are in the United States. We are a technology company that gives people the power to share their lives and experiences in an authentic and trusted environment making the world more open and connected. Facebook's privacy settings give users control over how they share their information allowing them to choose the friends they accept, the affiliations they choose, and how their information is shared with their friends, and, if they desire, the world at large.

Today, I would like to make four key points. First, Facebook's user centric approach to privacy is unique, innovative, and empowers consumers. Our privacy centric principles are at the core of our advertising model. Second, in offering its free service to users, Facebook is dedicated to developing advertising that is relevant and personal without invading users' privacy, and to give users more control over how their personal information is used in the online advertising environment. Third, we primarily achieve these objectives by giving users control over how they share their personal information that model real world information sharing and providing them transparency about how we use their information in advertising.

Fourth, the Federal Trade Commission's behavioral advertising principles recognize the important distinctions made by Facebook in its ad targeting between the use of aggregate, non-personally identifiable information that is not shared or sold to third parties versus other sites and companies' surreptitious harvesting, sharing, and sale of personally identifiable information to third party companies. Facebook understands that few of us want to be hermits sharing no information with anyone, nor do many of us want to share everything with everyone, though some do want that. Most people seek to share information with friends, their family, and others that they share a social context with on a regular basis seeking to control who gets our information and how they have access to it. People come to Facebook to share information. We give them the technological tools to manage that sharing.

Contrary to some popular misconceptions, full information on Facebook users isn't even available to most users on Facebook let alone all users of the Internet. If someone is searching for new friends on Facebook all that you might see about other users who are not yet her friends would be the limited information that those users have decided to make available. Most of our users choose to limit what profile information is available to non-friends. They have extensive and precise controls available to choose who sees what among their networks and friends as well as tools that give

them the choice to make a limited set of information available to search engines and other outside entities.

We are constantly refining these tools to allow users to make informed choices. Every day use of the site educates users as to the power they have over how they share their information and user feedback informs everything that we do. Facebook is transparent with our users about the fact that we are an advertising-based business and we explained to them fully the uses of their personal data that they are authorizing by interacting with Facebook either on facebook.com or on the over 10,000 Facebook connect sites throughout the web. Ads targeted to user preferences and demographics have always been part of the advertising industry. The critical distinction that we embrace in our advertising policies and practices and that we want this committee to understand is between the use of personal information for advertisements in personally identifiable form, and the use, dissemination or sharing of information with advertisers in non-personally identifiable form.

Users should choose what information they share with advertisers. This is a distinction that few companies make and Facebook does it because we believe it protects user privacy. Ad targeting that shares or sells personal information to advertisers in name, e-mail or other contact information without user control is materially different from targeting that only gives advertisers the ability to present their ads based on aggregate data. So to take in Dr. Felten's example, if you were to navigate to the social networking site, in his example if it were Facebook we would not be sharing with the ad provider that he was Edward Felten or that he likes jazz.

So on Facebook a feed is established where people know what they are uploading and receive timely reactions from their friends. The privacy policy and users' experience inform them about how advertising on the surface works. Advertising that enables us to provide the service for free to users is targeted to the expressed attributes of a profile and presented on the space on the page allocated for advertising without granting an advertiser access to any individual user's profile. Unless a user decides otherwise by directly and voluntarily sharing information with an advertiser, advertisers can only target Facebook advertisements against non-personally identifiable attributes of a user derived from profile data. Facebook builds and supports products founded on the principles of transparency and user control, and we thank you very much for the opportunity to present our philosophy on online advertising before this committee.

[The prepared statement of Mr. Kelly follows:]

Testimony of Chris Kelly

Chief Privacy Officer
Facebook

June 18, 2009

Before the U.S. House of Representatives Committee on Energy and Commerce

Subcommittee on Commerce, Trade, and Consumer Protection

Subcommittee on Communications, Technology, and the Internet

facebook

Testimony of Chris Kelly
Chief Privacy Officer
Facebook
June 18, 2009

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

Chairmen Waxman, Boucher and Rush, Ranking Members Barton, Radanovich and Stearns, and Members of the Subcommittees, thank you for the opportunity to address important privacy matters facing the online advertising industry.

I am Chris Kelly, Chief Privacy Officer of Facebook, an online site that serves more than 200 million active users worldwide, roughly 65 million of whom are in the United States. Facebook is a technology company that gives people the power to share their lives and experiences in an authentic and trusted environment, making the world more open and connected. From the founding of the company in a dorm room in 2004 to today, Facebook's privacy settings have sought to give users control over how they share their information, allowing them to choose the friends they accept, the affiliations they choose, and how those are presented to their friends and to the world at large.

Today, I would like to make four key points:

(i) Facebook's user-centric approach to privacy is unique, innovative and empowers consumers. Our privacy-centric principles are at the core of our advertising model.

(ii) In offering its free service to users, Facebook is dedicated to developing advertising that is relevant and personal without invading users' privacy, and to giving users more control over how their personal information is used in the online advertising environment.

(iii) We primarily achieve these objectives by giving users controls over how they share their personal information that model real-world information sharing and provide them transparency about how we use their information in advertising.

(iv) The FTC's behavioral advertising principles recognize the important distinctions made by Facebook in its ad targeting between the use of aggregate, non-personally identifiable information that is not shared or sold to third parties, versus other sites' and companies surreptitious harvesting, sharing and sale of personally identifiable information to third party companies.

I. Facebook and Privacy

From its founding, Facebook has understood that few of us want to be hermits, sharing no information with anyone. Nor do many of us want to share everything with everyone – though some do want that. Most people seek to share information with friends, family, and others they share a social context with on a regular basis, seeking to control who gets our information and how they have access to it. People come to Facebook to share information, we give them the technological tools to manage that sharing.

The statement that opens our privacy policy, a short plain-English introduction, is the best place to start this discussion. It reads:

We built Facebook to make it easy to share information with your friends and people around you. We understand you may not want everyone in the world to have the information you share on Facebook; that is why we give you control of your information. Our default privacy settings limit the information displayed in your profile to your networks and other reasonable community limitations that we tell you about.

Facebook follows two core principles:

1. You should have control over your personal information.
Facebook helps you share information with your friends and people around you. You choose what information you put in your profile, including contact and personal information, pictures, interests and groups you join. And you control the users with whom you share that information through the privacy settings on the Privacy page.

2. You should have access to the information others want to share.
There is an increasing amount of information available out there, and you may want to know what relates to you, your friends, and people around you. We want to help you easily get that information.

Sharing information should be easy. And we want to provide you with the privacy tools necessary to control how and with whom you share that information. If you have questions or ideas, please send them to privacy@facebook.com.

We implement these principles through our friend, network architectures, and privacy controls that are built into every one of our innovative products. Contrary to some popular misconceptions, full information on Facebook users isn't even available to most users on Facebook, let alone all users of the Internet. For example, if someone is searching for new friends on Facebook, all that she might

see about other users who are not yet her friends would be the limited information that those users have decided to make available. Many of our users choose to limit what profile information is available to non-friends. Users have extensive and precise controls available to choose who sees what among their networks and friends, as well as tools that give them the choice to make a limited set of information available to search engines and other outside entities.

We are constantly refining these tools to allow users to make informed choices whenever they are using the site. Everyday use of the site educates users as to the power they have over how they share their information, and user feedback informs everything we do.

One example conveys this concept better than any other. In February of this year, we looked to revise our Terms of Use, simplifying them to cut out as much legalese as possible and explain them in plain language. When we released a first version of our new terms, a blog misinterpreted our simplification of our copyright license, claiming that it meant we were seeking to own user content. The user reaction was predictably swift and severe, and we needed to choose among weathering the storm, revising the language, and introducing an entirely new process that would directly involve users in the governance of the site.

Our choice was to change our process in its entirety, building user input in through a notice and comment period modeled in part on the Federal government's rulemaking procedure, and instituting a user vote at the end of the process. This unprecedented innovation at this scale has led to a plain language set of governing documents for our site and greater user understanding about our rules and principles.

The comment period was very informative and led to useful revisions. When our users had the opportunity to vote on our new Statement of Rights and Responsibility, they were overwhelmingly affirmed with over 70% of those voting approving the new approach. In fact, we have committed to our users that any further changes to our critical site documents will be put out for discussion and, where certain activity thresholds are met, votes by our users. This is yet another way in which we allow our users to decide their own balance between what they keep private or make available to those with whom they wish to share information.

II. Privacy and Advertising on Facebook

A. Personally Identifiable and Non-Personally Identifiable Information

Facebook is transparent with our users about the fact that we are an advertising-based business, and we explain to them fully the uses of their personal data they are authorizing by interacting with Facebook either on Facebook.com or on the over 10,000 Facebook Connect sites throughout the Web. For instance, the

following explanation of how we use information for advertising has been a prominent part of our privacy policy for over three years:

Facebook may use information in your profile without identifying you as an individual to third parties. We do this for purposes such as aggregating how many people in a network like a band or movie and personalizing advertisements and promotions so that we can provide you Facebook. We believe this benefits you. You can know more about the world around you and, where there are advertisements, they're more likely to be interesting to you. For example, if you put a favorite movie in your profile, we might serve you an advertisement highlighting a screening of a similar one in your town. But we don't tell the movie company who you are.

Ads targeted to user preferences and demographics have always been part of the advertising industry. The critical distinction that we embrace in our advertising policies and practices, and that we want users to understand, is between the use of personal information for advertisements in personally-identifiable form, and the use, dissemination, or sharing of information with advertisers in non-personally-identifiable form. Users should choose what information they share with advertisers. This is a distinction that few companies make and Facebook does it because we believe it protects user privacy. Ad targeting that shares or sells personal information to advertisers (name, email, other contact oriented information) without user control is materially different from targeting that only gives advertisers the ability to present their ads based on aggregate data.

Many companies do not believe in this distinction, and to the extent that the Congress seeks to establish new legislation, it should be focused on these actors that undermine instead of enhance user control over personal data.

Most Facebook data is collected transparently in personally identifiable form– users know they are providing the data about themselves and are not forced to provide particular information. Sharing information on the site is limited by user-established friend relationships and user-selected networks that determine who has access to that personal information. Users can see how their information is used given the reactions of their friends when they update their profiles, upload new photos or videos, or update their current status.

On Facebook, then, a feedback loop is established where people know what they are uploading and receive timely reactions from their friends, reinforcing the fact they have uploaded identifiable information. The privacy policy and the users' experiences inform them about how advertising on the service works– advertising that enables us to provide the service for free to users is targeted to the expressed attributes of a profile and presented in the space on the page allocated for advertising, without granting an advertiser access to any individual user's profile.

Furthermore, advertising on Facebook is subject to guidelines designed to avoid any deceptive practices, and with special restrictions and review with respect to any advertising targeted at minors.

Unless a user decides otherwise by directly and voluntarily sharing information with an advertiser – for instance, through a contest –advertisers can only target Facebook advertisements against non-personally identifiable attributes of a user derived from profile data.

Products that provide personally identifiable information to advertisers without user permission, that rely on transforming non-personally identifiable information into personally identifiable information without notice and choice to users, or that rely on data collection that a user has no control over raise fundamentally different privacy risks and concerns than data sharing through Facebook.

Facebook builds and supports products founded on the principles of transparency and user control, where data may be collected directly from users in personally identifiable space but targeting is done based on aggregate or characteristic data in non-personally identifiable space. This approach respects users' privacy, it does not invade it. We believe other companies should follow our example of protecting privacy by giving users extensive control over their own data.

B. The Future of Advertising on the Web

Perhaps because our site has developed so quickly, Facebook may have sometimes been inartful in communicating with our users and the general public about our advertising products. We learned many lessons about the importance of user education and extensive control from the imperfect introduction of our Beacon product in 2007. As a result, Facebook continues to be dedicated to empowering consumers to control their information in both the noncommercial and the commercial context because we believe that should be the future of advertising.

Our next generation of Facebook interactions with third party (non-Facebook) websites, called Facebook Connect, empowers users to share content and actions with their friends throughout the Web using the Facebook infrastructure. Controls we built into this system serve users well and reflect our goals of transparency and user control.

As we look at serving targeted advertising on Facebook Connect and other sites, we publicly recommit ourselves to the critical goals of user understanding and empowerment, and the transparent approach to the use of data that remains under user control. We invite other companies to match our commitments, and welcome the Subcommittees' review of the privacy innovations we continue to implement at Facebook.

III. Federal Trade Commission Principles on Behavioral Targeting

Finally, we would like to reinforce our earlier positive comments about the Federal Trade Commission's ("FTC") leadership in addressing privacy concerns about how data are collected and shared online.

While our current Facebook Ads are materially different from behavioral targeting as it is usually discussed in that they are based on transparently collected data that users control, we applaud the FTC's desire to establish principles in this area. Given Facebook's goals of transparency and user control, the important corollary of ensuring appropriate security and the goal of providing users notice and choice with respect to service changes, the FTC principles describe the steps Facebook has already taken, and should guide where the rest of the industry should go.

We are pleased that the principles expanded and enhanced their discussion of the distinction between personally and non-personally identifiable information, and advertising based on those different types of information, from earlier versions. As these principles are implemented as standards for the industry, we look forward to working with other leaders to assure that users understand the implementation of innovative products and how users can exercise their own choice and control in these environments.

Thank you again, Chairmen, Ranking Members, and Subcommittee Members, for the opportunity to share our views. Facebook is very pleased to join you today, and looks forward to assisting the Subcommittees in their continuing review of these subjects.

Mr. RUSH. The chair thanks the gentleman. The chair now recognizes Mr. Chester for 5 minutes.

TESTIMONY OF JEFFREY CHESTER

Mr. CHESTER. I want to thank the chairs and ranking members and the members of the committee for their interest in privacy for holding this hearing and to support their efforts to, I think, help Americans get a fair digital data deal and that is what they deserve. Just very quickly before I make 4 points, I submitted my testimony in writing. It tries to lay out for the committee the broad parameters of the interactive advertising system as we know it in the United States, all the various elements that now are shaping this very powerful system so you can look at that if you want more information. I have been working on these issues for 15 years looking at online advertising, online marketing, digital communications. I last worked closely with the Commerce Committee back in 1998 when we led the campaign that established with your legislation the Children's Online Privacy Protection Act. Right now, that is the only online privacy law. It was a bipartisan effort. And what we did for kids, we now need to do for teens and adults.

Imagine the world, and this is the world that we have created and you have already spoken about it, both the chair spoke about it, Mr. Barton spoke about it, others have spoke about it. Imagine a world where every move, you are being watched, whatever contents you read, what you buy, how much you are willing to spend, and how much you are not willing to spend, where you go, what you like, what you don't like, all that being compiled. Outside databases being used to even build up this even larger profile of who you are. You include your race, whether you are a low income or middle class. They call it on the online ad industry digital fingerprints or user DNA but this very powerful system that is invisible and unaccountable to the average American is constantly collecting and refining and storing all this information and making claims and assumptions about you, your reputation without any accountability to you as the consumer let alone as the citizen.

That is the online advertising system today as we know it. It is different from traditional advertising because as you, yourself, described it is able to track you minute by minute, minute by second, and your information is being sold in online ad auctions in milliseconds. They know who you are and they are selling access to it, so it is an incredible system that we have created. And it is now meshed in almost everything we do online, watching online videos, even e-mail, doing searches, playing games. This broad date collection system is a digital data collection arms race going on as they build this incredibly sophisticated system. And I want to make it clear for my second point that our call for privacy and consumer protection rules isn't about undermining the role of online advertising and marketing. That has an important role to play. It is the underpinning, the foundation of our modern publishing system or really our new way of life in the digital age. We need to have online advertising and marketing, but we need to—and it is not about any particular company here or sense of companies. It is about the overall practices that the industry has created to collect all this information and to use all this information with these very powerful

multi-media, in their words, immersive online advertising services that are not understandable and controllable and definable by consumers.

I think to me it is very clear that you look at the issue of what is called sensitive data, which I am hoping you are going to work on, and in particular financial data. When you look at what happened during the recent financial crisis online advertising played a major role in encouraging people to take out those subprime mortgages. Online advertisers and mortgage companies were some of the biggest advertisers on the Internet during the boom period that led to this current crisis. People had no idea when they were taking out a mortgage or taking out a loan what exactly they were getting because this system was defining them in certain ways and making them various offers, once again, non-transparent to them, and as result, they, and I think we, have had to face the consequences.

That is just as with the financial system, we need some regulation here that puts the system into balance. Yes, they can try to build this business and we can be innovators, but, yes, consumers get to ensure what data is being used and how it is used, and they have a chance to change it if it is incorrect. So consumer groups around the country are calling on you to enact legislation as soon as possible to bring fair information principles up to the digital era. Self-regulation has failed. They have been working, with all due respect to my friends here, they have been working on self-regulation for 15 years and all you have is more and more data collected every minute. Americans shouldn't have to trade away their rights to control their information and have some autonomy in their affairs, whether it is buying a mortgage, looking up a prescription drug, buying a car or doing anything else without having to give their data up. There is a balance. I hope you will help us restore it. There is a win-win possible here. Thank you.

[The prepared statement of Mr. Chester follows:]

**Testimony to the House Committee on Energy and Commerce,
Subcommittee on Commerce, Trade, and Consumer Protection,
and the
Subcommittee on Communications, Technology, and the Internet**

For the hearing on
Behavioral Advertising: Industry Practices And Consumers' Expectations
June 18, 2009

Jeff Chester
Executive Director
Center for Digital Democracy

Summary of Testimony

Powerful techniques of data collection, analysis, consumer profiling and tracking, and interactive ad targeting have emerged across the online venues Americans increasingly rely on for news, information, entertainment, health, and financial services. Whether using a search engine, watching an online video, creating content on a social network, receiving an email, or playing an interactive video game, we are being digitally shadowed online. Our travels through the digital media are being monitored, and digital dossiers on us are being created—and even bought and sold. Behavioral Targeting is expected to become more widely used with online video, mobile phones, and online games and social networks, further expanding its data collection and targeting role. Such consumer profiling and targeted advertising takes place largely without our knowledge or consent, and affects such sensitive areas as financial transactions and health-related inquiries. Children and youth, among the most active users of the Internet and mobile devices, are especially at risk in this new media-marketing ecosystem.

Industry self-regulation, it is clear, has failed to offer meaningful protections to consumer privacy. So-called "Notice and Choice," which has been the foundation of the self-regulatory regime, has done nothing to stem the tide of increasing data collection and use—all without the genuinely informed understanding and consent of users. As with our financial system, privacy and consumer protection regulators have failed to keep abreast of developments in the area they are supposed to oversee. In order to ensure adequate trust in online marketing—an important and growing sector of our economy—Congress must enact sensible policies to protect consumers.

The foundation for a new law should be implementing Fair Information Practices for the digital marketing environment. Americans shouldn't have

to trade away their privacy and accept online profiling and tracking as the price they must pay in order to access the Internet and other digital media.

Chairman Boucher, Chairman Rush, Congressman Barton, Congressman Stearns, Congressman Radanovich, and Members of the Subcommittees, I am Jeff Chester, executive director of the Center for Digital Democracy (CDD). CDD is a non-partisan and not-for-profit organization based in Washington, D.C. Its mission is to help educate the public about the privacy, consumer protection, public health and competition issues related to the new digital media marketplace. CDD, along with our partner USPIRG, the federation of state Public Interest Research Groups, has played a major role at the Federal Trade Commission on data privacy and online marketing/consumer protection issues. In a series of complaints filed at the FTC in 2006, 2007 and earlier this year, CDD and U.S. PIRG pushed the commission to address the growing threats to consumer privacy and welfare that have emerged as a consequence of many online marketing practices, especially behavioral targeting.[1] I have worked on interactive marketing and consumer protection issues for more than a decade. As executive director of the Center for Media Education during the 1990's, I played a key role—along with Professor Kathryn C. Montgomery of American University—promoting privacy safeguards for children. That work eventually led to the passage, on a bi-partisan basis, of the Children's Online Privacy Protection Act of 1998 (COPPA).[2]

I want to commend the leadership of both committees, on both sides of the aisle, for their strong interest in ensuring U.S. consumers receive all the benefits of the digital age without having both their privacy and consumer welfare placed at risk. As I will explain in my testimony today, we are at a critical moment. Powerful techniques of data collection, analysis, consumer profiling and tracking, interactive ad creation

---

[1] Center for Digital Democracy and U.S. PIRG. Complaint and Request for Inquiry and Injunctive Relief Concerning Unfair and Deceptive Online Marketing Practices. Federal Trade Commission Filing. November 1, 2006 [Online]. Available at: http://www.democraticmedia.org/files/pdf/FTCadprivacy.pdf. Accessed March 26, 2009. Center for Digital Democracy and U.S. PIRG, "Supplemental Statement In Support of Complaint and Request for Inquiry and Injunctive Relief Concerning Unfair and Deceptive Online Marketing Practices," Federal Trade Commission Filing, 1 Nov. 2007, http://www.democraticmedia.org/files/FTCsupplemental_statement1107.pdf. Center for Digital Democracy and U.S. PIRG. Complaint and Request for Inquiry and Injunctive Relief Concerning Unfair and Deceptive Mobile Marketing Practices. Federal Trade Commission Filing. January 13, 2009 [Online]. Available at: http://www.democraticmedia.org/current_projects/privacy/analysis/mobile_marketing. Accessed March 23, 2009.

[2] For a detailed case study of the campaign to pass COPPA, see Chapter 4, "Web of Deception," in Kathryn C. Montgomery, *Generation Digital: Politics, Commerce, and Childhood in the Age of the Internet* (Cambridge, MA: MIT Press, 2007). I have continued to follow online marketing developments closely, including for my book, *Digital Destiny: New Media and the Future of Democracy* (The New Press, 2007).

and targeting have emerged across the online venues Americans increasingly rely on for news, information, entertainment, health, and financial services. Whether using a search engine, watching an online video, creating content on a social network, receiving an email, or playing an interactive video game, we are being digitally shadowed online. Our travels through the digital media are being monitored, and digital dossiers on us are being created—and even bought and sold. As *BusinessWeek* journalist Stephen Baker observed in his recent book, *The Numerati*, in his discussion of the behavioral advertising industry, "Late in the past century, to come up with this level of reporting, the East German government had to enlist tens of thousands of its citizens as spies. Today we spy on ourselves and send electronic updates minute by minute."[3]

Online Behavioral Targeting

Americans do not know much about what the industry calls the new "media and marketing ecosystem." The forms of advertising, marketing and selling that are emerging as part of the new media depart in significant ways from the more familiar commercial advertising and promotion we have seen in television, for example. In today's digital marketing system, advertising, editorial content, data collection, measurement, and content delivery are increasingly intertwined. As a major advertising industry report on the future of marketing in the digital era explained, "The influx of data into marketing has been one of the biggest changes to players across the landscape.... Advertising strategies, campaigns, and distribution are increasingly based on predictive algorithms, spreadsheets, and math.... Every Web page's individual views, every word typed in a search query box (also known as the 'database of consumer intentions'), every video download, and even every word in an e-mail may create one more data point that a marketer can leverage and use to more precisely target the audience...."[4]

Specifically, few U.S. consumers understand the power and intent of behavioral targeting, which, notes *eMarketer*, "segments the audience based on observed and measured data—the pages or sites users visit, the content they view, the search queries they enter, the ads they click on, the information they share on social internet sites and the products they put in online shopping carts. This data is combined with the time, length and frequency of visits.... Behavioral targets people, not pages. That is, behavioral uses the actions of a person to define its target, unlike contextual targeting, which serves ads based on a page's contents.... Behavioral information can also be merged with visitor demographic data—such as age, gender, and ZIP code.... Whether tracked by cookies or ISPs, the sort of user data

---

[3] Stephen Baker, *The Numerati* (New York: Houghton Mifflin Harcourt, 2008), p. 4.

[4] Edward Landry, Carolyn Ude, and Christoper Vollmer, "HD Marketing 2010: Sharpening the Conversation," Booz/Allen/Hamilton, ANA, IAB, AAAA, 2008, http://www.boozallen.com/media/file/HD_Marketing_2010.pdf.

that builds behavioral profiles takes in search queries, Web site visits, specific content consumed (such as clicks or playing a video), product shopping comparisons, product purchases and items placed in shopping carts but not bought."[5] U.S. spending for BT online advertising is predicted to grow dramatically to $4.4 billion by 2012 (up from "only $775 million in 2008").[6]

It is urgent, for two critical reasons, that Congress swiftly enact legislation that helps bring the concept of Fair Information Practices up to date in the digital age. First, we must ensure that the freedom of all Americans is protected in the online era. We shouldn't sanction the creation of a surveillance society where potentially many people—and government—can gain ongoing and comprehensive access to who we are and what we do. Our children and grandchildren, so-called "digital natives," are incorporating online media into almost everything they do, such as texting friends. We should protect their privacy and ensure we leave a digital civil liberties legacy for future generations.

Second, consumers must be in full control of their personal data, helping empower them as they increasingly rely on the Internet to engage in transactions, including those involving financial products and health concerns. As with the financial sector and a cause of the current economic crisis, regulators responsible for consumer privacy and online transactions have failed to adequately keep up with the directions of the marketplace—placing millions of Americans potentially at risk when engaged with online financial services (such as mortgages and loans). This and other hearings are essential to help inform the public that a whole new world has emerged for consumers: marketing is now fueled by the merging of online and offline databases, purposefully designed "immersive" interactive ad techniques, tracking and profiling users across the Internet, and the growing use of state-of-the-art "neuromarketing" techniques for digital marketing featuring (as Yahoo itself described in April 2009) "brain wave measurement, skin response testing, and eye tracking."[7]

---

[5] David Hallerman, "Behavioral Targeting: Marketing Trends," *eMarketer*, June 2008, pp. 2, 11. Personal copy.

[6] Hallerman, "Behavioral Targeting: Marketing Trends," p. 1.

[7] Chris Jaffe and Jill Strawbridge, "Measuring Online Ad Effectiveness Using Advanced Research Methods," Yahoo. Apr. 2009, l.yimg.com/a/i/us/ayc/aa_insights_advrschmeth.pdf. Microsoft, Google's DoubleClick, and many other digital marketing companies explain that digital marketing is different than traditional advertising, particularly for its ability to offer animation and multimedia-based "immersive" experiences. Such marketing techniques are designed to deeply engage the consumer with the content of the marketing message. See, for example, Microsoft Advertising, "Emotional Side of Digital Advertising," Oct. 2007, http://advertising.microsoft.com/uk/Emotional-Side-of-Digital-Adv; Microsoft Advertising, "Maximize Reach and results through Rich Media," http://advertising.microsoft.com/rich-media; DoubleClick, "DoubleClick Rich Media and Video," http://www.doubleclick.com/products/richmedia/index.aspx; Eyeblaster, "About Us," http://www.eyeblaster.com/Content.aspx?page=about_us (all viewed 14 June 2009). Such techniques are tied to data collection as well.

Protecting consumer privacy online is also vital if we are to protect consumers, who have already suffered massive financial losses and other personal hardships as a result of the recent financial debacle (and who face other risks, such as the growth of "ID Theft" and data security leaks). Mortgage loans, credit cards, and other financial products for consumers were—and are—being made available through an online marketing system that is non-transparent, unaccountable to individual users, and unfair. The equation must be balanced: consumer autonomy and privacy that can fairly contend with the tremendous clout online advertisers have today through data collection, profiling and "micro-targeting."[8] There is an urgency for action, as the current economic crisis is fostering an even greater reliance on the online medium by consumers. Google recently told advertisers in the United Kingdom that "the slowdown will speed up consumer use of digital technology...and greater use of the Internet."[9] We will see increased consumer online activity connected to critical financial transactions—from online shopping, banking, and bill paying to applying for loans and mortgage—that get to the very heart of our economy.[10] If we are to protect consumers from further personal financial loss, Congress should ensure that the online marketing system operates in a transparent and accountable manner.

I want to be clear that our call for privacy and other consumer protection rules related to data collection and online commerce isn't about undermining the role that advertising and marketing plays in our digital-based economy. Advertising and marketing has and will continue to play a critically vital role for our digital media. Advertising revenues are a crucial source of funding for online content. Marketing online has enabled a "long-tail" of electronic commerce, including from small businesses, to emerge and thrive. We should be proud of the impressive level of technological and business innovation from this sector. My concern about the growing threat to our privacy and related consumer protection issues stems not from the activities of a single—or even several—major companies in this sector. Rather, it is from the overall capability and direction of the online marketing industry when it comes to data collection marketing practices. It is precisely to ensure the growth of online marketing and advertising that consumer privacy must be protected. Consumers and citizens shouldn't be asked to agree to some form of

---

[8] Tom Agan, "Silent Marketing: Micro-targeting," Penn, Schoen and Berland Associates,www.wpp.com/NR/rdonlyres/4D3A7EB2-9340-4A8D-A435-FDA01DD134D0/0/PSB_SilentMarketing_Mar07.p

[9] Google, "Speeding Up in the Slowdown," 2008, personal copy.

[10] "The April 2009 "comScore State of Online Banking" report, for example, "found that the number of online banking customers continued to grow strongly in 2008 despite the turbulent financial environment. The growth was fueled by banks' aggressive customer acquisition strategies and heightened financial interest among online banking customers wanting to keep a closer eye on their personal finances." comScore, "Number of U.S. Online Banking Customers Continues to Grow Despite Challenging Financial Environment," 21 Apr. 2009, http://www.comscore.com/Press_Events/Press_Releases/2009/4/2009_State_of_Online_Banking_Report (viewed 21 May 2009).

trade-off where they lose their privacy and protections in order to see a marketplace financially grow. Without ensuring meaningful policies that will promote consumer trust, online marketing in the U.S. will be undermined by a lack of confidence.

Some in the online ad industry appear to suggest that any legislative attempt to place consumers in charge of their online data would undermine the economic role of the Internet media. But I believe that by legislatively creating a system where consumers can be assured that their data are protected and transactions are structured to further empower them, trust and confidence in our online marketplace will grow and thrive. I firmly believe that we can protect privacy and also see the online marketplace and medium prosper.

Along these lines, I asked Professor Joseph Turow, Ph.D., of the Annenberg School of Communication, University of Pennsylvania—one of the country's leading independent experts on digital marketing—to respond to the alarmist calls from some industry groups about the impact of a law protecting privacy online. Professor Turow explained that:

> Far from destroying the opportunity for revenue in the digital world, a marketplace distinguished by information transparency and customer prerogatives can help move businesses in new, profitable directions. The reason lies in the relation between consumer trust and the brand. It is a well-accepted proposition that customer trust is at the core of a brand's profitability. In the world of material goods, customer trust primarily centers on two attributes—the **accuracy** of claims about the product and whether it **works** well. In products of the digital age that involve customer data, trust centers on those two attributes as well as two others: **transparency** regarding a company's specific uses of a customer's information and the customer's **prerogative** to include, withdraw, or otherwise limit the use of that information. While some executives fear that providing customers with information transparency and prerogatives will alienate customers and reduce profits, it is highly likely that just the opposite will happen. Moreover, an appropriate regulatory environment can encourage a new market that helps consumers make sense of, and guide, the streams of data about them.[11]

Studies Show the Public is Concerned about Privacy Online

Surveys conducted by reputable organizations have highlighted two important findings: Consumers highly value data privacy, and consumers are confused about

---

[11] Personal correspondence, 14 June 2009. Professor Turow is the author of several books, including *Niche Envy: Marketing Discrimination in the Digital Age* (Cambridge, MA: MIT Press, 2008).

company protections of customer privacy. Few consumers really understand the data collection system and targeted advertising environment online. The University of Southern California's Center for the Digital Future found in its eighth annual "Surveying the Digital Future" project that "almost all respondents continue to report some level of concern about the privacy of their personal information when or if they buy on the Internet."[12] A poll from the Consumer Reports National Research Center found "72 percent are concerned that their online behaviors were being tracked and profiled by companies."[13] Surveys by the University of Pennsylvania's Annenberg School of Communication and the University of California at Berkeley Law School's Samuelson Law, Technology & Public Policy Clinic also found confusion about customer data and customer privacy protections offered by businesses.[14] A 2008 Harris Interactive poll found that U.S. consumers "are skeptical about the practice of websites using information about a person's online activity to customize website content."[15]

A June 2009 study from the UC Berkeley's School of Information found that

> ... most of the top 50 websites collect information about users and use it for customized advertising. Beyond that, however, most contained unclear statements (or lacked any statement) about data retention, purchase of data about users from other sources, or the fate of user data in the event of a company merger or bankruptcy.
>
> Sharing of information presents particular problems. While most policies stated that information would not be shared with third parties, many of these sites allowed third-party tracking through web bugs. We believe that this practice contravenes users' expectations; it makes little sense to disclaim formal information sharing, but allow functionally equivalent tracking with

---

[12] USC Annenberg School for Communication, "Annual Internet Survey by the Center for the Digital Future Finds Large Increases in Use of Online Newspapers," press release, 28 Apr. 2009, http://www.scribd.com/doc/15015797/USC-Annenberg-School-Digital-Future-2009-Highlights (viewed 14 June 2009).

[13] Consumers Union, "Consumer Reports Poll: Americans Extremely Concerned About Internet Privacy; Most Consumers Want More Control Over How Their Online Information Is Collected & Used," press release, 25 Sept. 2008, http://www.consumersunion.org/pub/core_telecom_and_utilities/006189.html (viewed 14 June 2009).

[14] Chris Jay Hoofnagle and Jennifer King, "Research Report: What Californians Understand About Privacy Online," 3 Sept. 2008, http://www.law.berkeley.edu/clinics/samuelsonclinic/files/online_report_final.pdf (viewed 14 June 2009).

[15] Harris Interactive, "Majority Uncomfortable with Websites Customizing Content Based Visitors Personal Profiles," press release, 10 Apr. 2008, http://www.harrisinteractive.com/harris_poll/index.asp?PID=894 (viewed 14 June 2009).

third parties.[16]

The Evolving World of Online Marketing and Data Collection

Today, we are witnessing a dramatic growth in the capabilities of marketers to track and assess our activities and communication habits on the Internet.[17] Advertisers and marketers have developed an array of sophisticated and ever-evolving data collection and profiling applications, honed from the latest developments in such fields as semantics, artificial intelligence, auction theory, social network analysis, data-mining, and statistical modeling. Behavioral targeting (BT), the online marketing technique that analyzes how an individual user acts online so they can be sent more precise marketing messages, is just one tool in the interactive advertisers' arsenal. Social media monitoring, so-called "rich-media" immersive marketing, new forms of viral and virtual advertising and product placement, and a renewed interest (and growing investment) in neuromarketing, all contribute to the panoply of approaches that also includes BT. Behavioral targeting itself has also grown more complex. That modest little "cookie" data file on our browsers, which created the potential for behavioral ads, now permits a more diverse set of approaches for delivering targeted advertising. We are being intensively tracked on many individual websites and across the Internet. Behavioral targeting and related technologies may provide "marketing nirvana," as one company explained, but it leaves consumers unaware and vulnerable to an array of marketing communications that are increasingly tied to our financial and health activities.[18]

Advances in the capabilities of digital advertising are being made through a variety of initiatives. For example, Microsoft has established its adLab, with offices in Beijing, Redmond, Washington, and other locations, to work on behavioral targeting and other techniques. Yahoo! Labs in Bangalore works on a number of topics related to "advertising sciences." Google and the leading global advertising company WPP just established a grant program for academics to "to improve understanding and practices in online marketing."[19]

---

[16] "Consumer Advocacy Group Comments In the Matter of a National Broadband Plan for Our Future," Center for Digital Democracy, Privacy Rights Clearinghouse and U.S. PIRG, FCC Docket 09-51, June 2009, http://www.democraticmedia.org/node/405 (viewed 14 June 2009).

[17] For a useful online illustration on the data collection and targeting capabilities of online ad networks, see *Advertising Age's* "Ad Networks+ Exchanges Guide. 2009. http://brandedcontent.adage.com/adnetworkguide09/lobby.php?id=2 (viewed 14 June 2009).

[18] "The Rise of On-site Behavioral Targeting," http://www.omniture.com/offer/281 (viewed 14 June 2009).

[19] Microsoft, "adCenter Labs—Innovations in Digital Advertising," http://adlab.microsoft.com/; .Yahoo! Labs Bangalore, "Advertising Sciences," http://bangalore.yahoo.com/labs/asceinces.html; "Google and WPP Marketing Research Awards Program bestows 11 grants," press release, 18 Mar. 2009, http://www.wpp.com/wpp/press/press/default.htm?guid=%7Be0af399a-8450-408c-8ba8-c35d31dae88c%7D. Advances in digital advertising, including through data mining, artificial

One of the not-so-subtle ironies of the debate about behavioral advertising and privacy is that when marketers are grilled by regulators, they claim BT isn't really targeted to an individual and is relatively harmless. But what they tell each other reveals a medium with a powerful punch. The U.S. Interactive Advertising Bureau, the industry's principal trade and lobbying group, defines behavioral targeting as *"A technique used by online publishers and advertisers to increase the effectiveness of their campaigns. Behavioral targeting uses information collected on an individual's web browsing behavior such as the pages they have visited or the searches they have made to select which advertisements to be displayed to that individual. Practitioners believe this helps them deliver their online advertisements to the users who are most likely to be influenced by them."*[20]

Among the many companies harnessing the power of behavioral targeting to fuel their online ad efforts is Yahoo! In a 2007 presentation to UK advertisers, Yahoo touted its behavioral targeting as a form of "intelligent user profiling." Explaining that it captures user "DNA" from "registration and behaviours" (including online activities such as page views, ads clicked, search queries, and search clicks), Yahoo uses this information to fuel its behavioral targeting. Behavioral targeting company Audience Science acknowledges the "massive amounts of data" it has available "to gain consumer insights on an individual level."[21]

In addition to targeting users on individual websites, BT also permits tracking of individual users across hundreds or more sites. Called retargeting, one company specializing in that approach explains it is *"able to deliver your message to visitors after they have left your site as they surf the Web. Your ads will appear to them as they surf their favorite internet sites—everything from popular news sites, social networking sites, to various blogs and informational sites. These are not pop-ups; these*

---

intelligence, and social media "sentiment" analysis, are supported by online marketers such as Microsoft, Google, and Yahoo, at various specialized academic conferences. See, for example, the upcoming Third Annual International Workshop on Data Mining and Audience Intelligence for Advertising," 28 June 2009, in Paris, http://adlab.microsoft.com/adkdd2009/ (all viewed 14 June 2009).

[20] Interactive Advertising Bureau, "Glossary of Interactive Advertising Terms v. 2.0," http://www.iab.net/media/file/GlossaryofInteractivAdvertisingTerms.pdf. The US IAB counterpart in the United Kingdom defines behavioural targeting as "A form of online marketing that uses advertising technology to target web users based on their previous behaviour. Advertising creative and content can be tailored to be of more relevance to a particular user by capturing their previous decision making behaviour (eg: filling out preferences or visiting certain areas of a site frequently) and looking for patterns." Internet Advertising Bureau, "Jargon Buster A-D," http://www.iabuk.net/en/1/glossaryatod.html (both viewed 14 June 2009).

[21] "AudienceScience CEO Hirsch Says Real-Time Bidding Enables True Value in Media," AdExchanger.com, 13 Mar. 2009, http://www.adexchanger.com/ad-networks/behavioral-targeting-audiencescience/ (viewed 14 June 2009). For more examples of behavioral marketing practices, see my blog: http://www.democraticmedia.org/jcblog/?cat=37.

are advertisements that customers would normally see as they visit these webpages; only instead of a random ad being displayed, a targeted ad specifically for them will be shown. Think of it as following a customer out the front door of your store and asking if they saw the sale rack on the back wall. You appear to them again in the right place—at the right time. You will stay top of mind and customers will come back to your site and purchase."[22]

The use of retargeting also raises issues related to potential price discrimination, where certain consumers are offered "better deals" because they are seen as more long-term, lucrative customers. In recent presentations, Datran Media explained that it matches "*verified* offline demographic and lifestyle data with millions of online users" to deliver its targeted advertising.[23] But it also noted that for "Retargeting, Not all customers are equal," describing one consumer in a "low income bracket" who spends only $24.00 over an eight-month period versus "Customer Type B" in the "middle income bracket," who spends $140.00 over three years." Such a system—where one user is determined through a variety of variables to be a better prospect than another and is offered different deals—raises a number of concerns about accountability, transparency, fairness, etc.[24]

Behavioral targeting is growing. A recent study by Datran Media, which "surveyed more than 3,000 industry executives from Fortune 1,000 brands and interactive agencies, found that 65% of marketers use or plan to use behavioral targeting."[25] More than half of the 1,200 marketers surveyed by Marketing Sherpa said they would increase their spending for behavioral targeting in 2009.[26] BT is expected to become widely used with online video, mobile phones, and online games and virtual worlds, further expanding its data collection and targeting role.[27]

---

[22] Fetchback, "Retargeting," http://www.fetchback.com/retargeting.html (viewed 14 June 2009).

[23] Scott Knoll, "The Future of Behavioral Targeting," 18 Dec. 2008, http://s3.amazonaws.com/thearf-org-aux-assets/downloads/cnc/online-media/2008-12-18_ARF_OM_Datran_Media.pdf (viewed 14 June 2009).

[24] Knoll, "The Future of Behavioral Targeting." See also "Always Make a Good Impression: Understanding Household & Behavioral Targeting to Maximize Your Media Buys," 1 Oct. 2008, http://success.datranmedia.com/webinars/ (viewed 15 June 2009)

[25] "Datran Media Announces Third Annual Marketing Survey Results," press release, 27 Jan. 2009, http://corporate.datranmedia.com/newsandpress/press.php?id=01272009 (viewed 14 June 2009).

[26] Marketing Sherpa, "New Data: Year-End Survey Shows ROI and Budgets by Tactic," 4 Feb. 2009, http://www.marketingsherpa.com/article.php?ident=31037 (subscription required). Nearly half in this survey said they would spend more on ads fostering greater interactivity (so-called "rich media").

[27] "Behavioral Targeting Ad Spend Poised to Grow, with Help from Online Video" *Marketing Vox*, 23 June 2008, http://www.marketingvox.com/behavioral-targeting-ad-spend-poised-for-growth-with-help-from-online-video-039399/; "Yahoo to Bring Behavioral Targeting to Mobile," *Marketing Vox*, 21 May 2009, http://www.marketingvox.com/yahoo-to-bring-behavioral-targeting-to-mobile-044141/; "Behavioral Targeting in Second Life," Advertising Lab, 28 Apr. 2007,

The Role of BT in Finance

Perhaps the most cautionary tale about the need to protect consumer privacy online arises when examining the role of online advertising and the financial market. By 2011, 101 million adults will be banking online—many even using their mobile devices to engage in personal financial transactions.[28] As evidence of the plight Americans feel today about their financial losses, it is perhaps telling to examine how the crisis has effected what they are searching for online. According to online market research company comScore, last December there were "searches using the term 'unemployment' (up 206 percent to 8.2 million searches) and 'unemployment benefits' (up 247 percent to 748,000 searches)... terms relating to personal asset situations, including 'mortgage' (up 72 percent to 7.8 million searches), 'bankruptcy' (up 156 percent to 2.6 million searches), and 'foreclosure' (up 67 percent to 1.4 million searches)."[29]

During the height of the housing boom, the top-25 mortgage companies by advertising spending dolled out enormous sums on online advertising, especially display advertising. Four mortgage or financial companies were in the top ten of online advertising spending in August 2007, according to Nielsen: Low Rate Source (#1), Experian Group (#3), InterActive Corp (#4) [which then included Lending Tree.com] and Countrywide Financial Corporation (#5).[30] Consumers were faced with increasing expenditures by mortgage and loan companies for online marketing. For example, from 2005 to 2007, online mortgage services companies Countrywide Financial and LowRateSource increased their online advertising spending from $18.3 to $35.5 and $17.9 million to $51.7 million, respectively.[31] Meanwhile, mortgage companies, anxious to have a prominent place in search engine

---

http://adverlab.blogspot.com/2007/04/behavioral-targeting-in-second-life.html (all viewed 14 June 2009).

[28] Lisa E. Phillips, "Banking and Bill Paying Online: Chasing Those Digital Dollars," May 2007, http://www.emarketer.com/Report.aspx?code=emarketer_2000412. For mobile applications, see "Banking and Payments," *Mobile Marketer*, http://www.mobilemarketer.com/cms/news/banking-payments.html (both viewed 14 June 2009).

[29] "Americans' Online Search Behavior Points to Significant Increase in Personal Financial Turmoil," press release, 24 Feb. 2009, http://www.comscore.com/Press_Events/Press_Releases/2009/2/Economic_Search_Terms (viewed 14 June 2009).

[30] "Nielsen/Netratings Reports Topline U.S. Data for August 2007," www.nielsen-online.com/pr/pr_070910.pdf; Peter Kafka, "What Mortgage Crisis? Financial Ads Keep Pouring Online," *Silicon Alley Insider*, 10 Sept. 2007, http://www.businessinsider.com/2007/9/what-mortgage-c (both viewed 14 June 2009).

[31] Nielsen/NetRatings Report, Top 10 Advertisers by Estimated Spending, December 2006; April 2007; and August 2007.

advertising, bid up search terms like "refinancing mortgage" and "mortgage refinance." Among the "highest paying keywords" for Google in 2006 involved mortgage related inquires, with the "most aggressive users of keyword advertising" done by "asbestos lawyers, ambulance chasers, and mortgage brokers."[32]

The role of online lead generation (so-called "trigger leads") and the use of behavioral targeting for mortgages and other loans represent a potentially critical threat to the privacy of digital consumers, whose data are used without their clear understanding, let alone control, of such surveillance. For example, Lightspeed Research promises marketers a "full wallet view across customers' many financial services relationships," providing "unparalleled insight into consumers' use of credit, debit, banking and alternative payment products. We passively gather information from their financial accounts and merge it with third-party behavioral datasets, survey-based attitudinal insights, and industry expertise."[33] Such commingling of online and off-line data, providing veritable strip searches of consumers' economic status and marketplace behavior, has become commonplace, thanks to companies such as Targusinfo. "With the largest repository of US offline consumer information," the company declares, "Targusinfo is uniquely positioned to take online targeting to the next level.... Its data repository is updated ten times daily and incorporates millions of data points across more than 100 dynamically changing data sources."[34] "...Targusinfo has built a foundation of data from the nation's telecommunications providers," the company admits, "making our information exceptionally precise, relevant and actionable. Drawing from a proprietary network of more than 90 data sources, Targusinfo uses patented processes to link together the most complete and accurate name, address and phone data possible."[35] So-called "trigger leads," part of the online industry's "lead generation" business, are also a part of the online ad environment, giving marketers

---

[32] Financial services companies were reported to having "doubled their spending on Internet advertising during the past four years," with predictions of further significant increases. "Online Spending to Balloon at Financial Co.s," *Mortgage Advertising Insider*, 5 June 2007, http://www.mortgagedaily.com/NewsAlertArchives/AdNewsletter060507.html; Bernstein Research estimated 30 percent of online ad spending for 2008 would from finance, real estate ad insurance. Laurie Sullivan, "Bernstein: Online Ad Revenue To Grow," *Online Media Daily*, 11 Aug. 2008, http://www.mediapost.com/publications/?fa=Articles.showArticle&art_aid=88244 (both viewed 14 June 2009); "Most expensive Google ad keywords listed." Cory Doctorow. Boingboing.com. 26 March 2006. http://www.boingboing.net/2006/03/26/most-expensive-googl.html (viewed 16 June 2009).

[33] Lightspeed Research, Financial Services Brochure, http://www2.lightspeedresearch.com/uploads/Financial_Services_Brochure.pdf (viewed 22 May 2009).

[34] Targusinfo, "Taking Online Targeting to the Next Level," Mar. 2009, http://marketing.targusinfo.com/AdAdvisorLearningCenter.html (viewed 22 May 2009).

[35] Kim Garner, "How to Master Customer Acquisition: On-Demand Lead Scoring," Apr. 2008, http://www.targusinfo.com/documents/LeadScoring.pdf (viewed 22 May 2009).

the ability to target consumers based on the financial activity at "near real time speed and precision."[36]

Omniture, an online marketing and Web analytics company that has worked with some of the largest subprime lenders in the mortgage industry, including Countrywide Financial, is a leader in behavioral targeting. Through its "foundational product," SiteCatalyst, the company provides "actionable, real-time intelligence" about the online behavior of users visiting their websites.[37] Omniture's use of behavioral targeting illustrates how this powerful approach is different from more traditional direct marketing. It explains that

> On-site Behavioral Targeting leverages highly automated technology that takes advantage of the same Web analytics data you are most likely already collecting, such as referring site, referring search engine and keyword phrase, time and day of visit, machine properties such as IP address and browser settings, along with complete individual visitor click-stream data. The system efficiently organizes the anonymous data to build individual visitor profiles containing the hundreds of data variables that occur during a visitor's visit to a Web site, each with some small amount of predictive value. Highly sophisticated mathematical models then interpret these variables in real-time and assemble together their collective predictive value to determine exactly which piece of content or promotion is most likely to engage each visitor, and then serves that content while the visitor is still on the site, keeping track of the entire context of each piece of served content. The On-site Behavioral Targeting system then measures if the visitor responded to the served content in the manner predicted. By efficiently learning in real time from any differences between the predicted response behavior and actual response behavior, the system continuously makes itself smarter for the next decision....

---

[36] See, for example, Equifax Marketing Services, "TargetPoint Acquisition," www.equifaxmarketingservices.com/pdfs/TargetPoint-Acquisition-F06.pdf; Equifax Marketing Services, "High-Tech Industry," http://www.equifaxmarketingservices.com/high-tech-industry.htm. One online marketing explained why online lead generation (OLG) is preferable to an offline approach: "With OLG, marketers are guaranteed to be getting new, fresh data and they don't have to worry about its relevance—it is guaranteed to be up to date. As the data is brand-new and unique to them, it won't have been sitting in a database for years while the person could have moved their house, changed telephone numbers or even changed their name. And due to the rigorous data-cleansing processes of Online Lead Generation, every lead is guaranteed to be fully contactable—there are no 'dead leads,' and all the contact details are fully checked." Christopher Petix, "Economy Calls For Online Lead Generation," *Online Media Daily*, 10 Feb. 2009, http://www.mediapost.com/publications/?fa=Articles.showArticle&art_aid=99943 (all viewed 14 June 2009).

[37] Omniture, "Omniture SiteCatalyst 14: Real-Time, High-Performance Analytics & Reporting," http://www.omniture.com/offer/170 (registration required).

> 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, in order to achieve a desired and measurable commercial objective; such as increasing revenue, conversion, or click-through. It then measures its effectiveness and reports back the lift and yield that it delivers. On-site Behavioral Targeting is marketing nirvana in many ways, as it closes the loop in real-time while the visitor is still on your Web site.[38]

Bankrate.com actively engages in behavioral targeting, explaining that "a consumer comes to Bankrate.com and reads three home equity articles, calculates the benefits of a home equity loan vs. a HELOC and looks at rates for a $50k home equity loan. This consumer has shown tremendous interest and intent in securing a home equity product. As an advertiser, you now have the ability to continue communicating with this consumer across hundreds of web sites."[39]

Bankrate.com's website places tracking cookies in online users' browsers, which then tracks pages later visited by them. Bankrate.com consumers who view "a mortgage story, rate table, or calculator within the last 120 days will be tagged and placed in the Mortgage Behavioral Targeting Bucket/Segment." When such a consumer visits a site within the Bankrate.com's behavioral targeting network, they will receive mortgage advertising. Bankrate.com offers behavioral targeting-enabled services for Mortgages, Home Equity, Credit Cards, and Deposits (CDs/Investment/Checking/Savings). In its Web page explaining "Why Behavioral Targeting," Bankrate.com notes that "Now you can expand upon this finite target and follow these users with your message once they've left the Bankrate site, but while they are still very much in-market...."[40]

The Emerging Array of Behavioral Marketing Applications, including "Predictive" BT

BT's ability to lock in individual users is also being fueled by connections to offline databases, as well as other profiling technologies. For example, Acxiom, the marketing database giant, now offers a range of targeting tools for online marketing,

---

[38] Omniture, "The Rise of Onsite Behavioral Targeting," http://www.omniture.com/en/products/conversion (registration required).

[39] "Behavioral Targeting FAQs," Bankrate.com, http://www.bankrate.com/mediakit/ad-behavioral-faq.asp (viewed 14 June 2009).

[40] "Behavioral Targeting," Bankrate.com, http://www.bankrate.com/mediakit/ad-behavioral.asp; "Behavioral Targeting: How Does it Work?" Bankrate.com, http://www.bankrate.com/mediakit/ad-behavioral-how.asp (both viewed 14 June 2009).

including on websites, mobile phones and email.[41] It's "Relevance-X"™ product, Acxiom explains, allows it to leverage "our expertise in consumer information and consumer behavioral segmentation to help marketers target and deliver personalized advertising messages.... Relevance-X helps you deliver the right message to the right audience where consumers are today—online.... Unlike traditional consumer segmentation systems, PersonicX is built and applied at the consumer household level, not at a ZIP Code™ or block group."[42]

Online targeting now also involves the use by marketers of sophisticated techniques that merge user data with information about our psychological or emotional behaviors.[43] For example, Mindset Media "lets advertisers define their targets on 21 standard elements of personality and then reach those targets on a mass scale in simple online media buys.... A MindsetProfile will identify the psychographics that drive your brand, your category, and even your competitors." Such targeting is available over one ad network that reaches "150 million unique viewers each month across more than 1,500 sites globally."[44]

So-called "Predictive Behavioral Targeting" has emerged, which is described as a "technology that tries to target ads not only based on people's click behavior but also on predictions about their interests and future behavior." Engaging in "real-time" data tracking and analysis, predictive BT "learns from user behavior in realtime" and can be "exploited" for interactive marketing.[45] One U.S. predictive

---

[41] Explaining its acquisition of behavioral re-targeting company EchoTarget, an Acxiom executive noted that the "acquisition goes beyond the current behavioral targeting paradigm to give clicks context, leveraging the most comprehensive data assets in the industry by combining proven direct marketing techniques segmenting individuals based on demographics, shopping patterns and lifestyle factors with the behavioral-based approaches of online targeting." Giselle Abramovich, "Acxiom Enters Digital Advertising with Acquisition of EchoTarget," *DM News*, 20 Sept. 2007, http://www.dmnews.com/Acxiom-enters-digital-advertising-with-acquisition-of-EchoTarget/article/98540/ (viewed 14 June 2009).

[42] Acxiom, "Acxiom Relevance-X," http://www.acxiom.com/PRODUCTS_AND_SERVICES/DIGITAL/RELEVANCE-X/Pages/Relevance-X.aspx; Acxiom, "The Power of Data: Acxiom Relevance-X Fact Sheet," http://www.acxiom.com/SiteCollectionDocuments/website-resources/pdf/Fact_Sheets/Relevance-X_FactSheet.pdf (both viewed 14 June 2009).

[43] For more on developments in the behavioral targeting market, see, for example, Behavioral Insider, http://www.mediapost.com/publications/?art_type=31&fa=Archives.showArchive; other useful sources include iMedia Connection, http://imediaconnection.com, and ClickZ, http://www.clickz.com/ (all viewed 14 June 2009).

[44] Mindset Media, "Media with Attitude," http://www.mindset-media.com/; Mindset Media, "Our Products," http://www.mindset-media.com/advertisers/products/; Mindset Media, "MindsetProfile, http://www.mindset-media.com/advertisers/products/profiles/ (all viewed 14 June 2009).

[45] Predictive Behavioral Targeting, "What is PBT?" http://www.predictive-behavioral-targeting.com/what-is-predictive-behavioral-targeting/. For an animated overview of predictive behavioral targeting, see nugg.ad, http://www.nugg.ad/en/products/flash.html (both viewed 14 June 2009).

behavioral marketer explained that its new "Precision Profiles" product uses "...a wider spectrum" of data for such targeting, "including web browsing, ad interaction, search and shopping behavior" that "results in more granular profiles."[46]

Behavioral targeting is just one tool used by online marketers to gather information on users. Online marketers employ an array of interrelated techniques to target individual users, as well as to collect (or facilitate the collection of) consumer data.[47] Semantic-based profiling (based on the tagging and analysis of Web pages) is also used. For example, Collective Media's "advanced audience behavior targeting" can use a "contextual classification engine" that analyzes "each page for the presence of over 2 million words and word combinations, and [uses] this analysis to categorize and/or tag pages into over 200,000 hierarchical categories.... Personifi's uniquely powerful ad optimization solution observes all available behavioral, contextual, demographic and other data to determine the most effective ad for each impression.... Personifi leverages this understanding to deliver the most relevant ads to individual users at the optimal times. Ad recommendations are continually optimized in real time based on observed behaviors and responses."[48]

The collection of individual data to create more personalized online experiences, while potentially useful, raises privacy and consumer protection issues. As data are collected, a user's online experience is altered, with pages being tailored to an "individual user's characteristics and behaviors." Users have no idea, for example, that x+1's "Predictive Optimization Engine (POE)" is part of a "predictive marketing platform that utilizes automated, real-time decision-making to improve the scale and efficiency of the online marketing process.... [It] leverages sophisticated mathematical models to make optimal segmentation and targeting decisions on website and in external media campaigns. POE™ derives actionable decisions from massive amounts of complex data. Using a wide variety of data sources, POE™ profiles end-users and anonymously tracks their online behavior and responsiveness. It then identifies patterns in visitor characteristics and their

---

[46] "ValueClick Media Launches Predictive Behavioral Targeting," press release, 21 July 2008, http://phx.corporate-ir.net/phoenix.zhtml?c=84375&p=irol-newsArticle&ID=1177051 (viewed 14 June 2009).

[47] To see how major online marketers offer an array of targeting options, including behavioral and mobile marketing, see, for example, AOL Platform A, "Audience Targeting," http://www.platform-a.com/advertiser-solutions/audience-targeting; Microsoft Advertising, "Ad Solutions," http://advertising.microsoft.com/ad-solutions; and Yahoo! Advertising, "Advertiser & Agency Solutions," http://advertising.yahoo.com/advertisers/ (all viewed 14 June 2009).

[48] Collective Media, "Targeting by Behavior," http://www.collective.com/targeting#behavior; Personifi, "Ad Network Optimization," http://www.personifi.com/ad_networks_optimization.html; Personifi, "Ad Network: Contextual," http://www.personifi.com/ad_networks_contextual.html; Personifi, "Ad Network Classification," http://www.personifi.com/ad_networks_classification.html (all viewed 14 June 2009).

response activity and ultimately determines the best content and offer to display."[49] As we will explain later, the use of "anonymous" by so many marketers is at odds with the tremendous and undisclosed data collection that is increasingly shaping our experiences online.

The self-learning capabilities of contemporary interactive ad systems also raise important privacy and consumer welfare concerns. For example, "Meaning-Based Marketing" by one company "forms an understanding of the sentiment and context of all customer interactions, including social media, user-generated content and user interactions." It "creates a targeting system... based on deep profiles, sentiment, behavior, all major types of customers attributes, and the content and concepts."[50]

An array of other data tools has emerged that is shaping the experience—and the deals and offers—available to the American consumer. For example, "Using web analytics," boasts online marketer Coremetrics, "businesses can clearly see a customer's path from an email opened to an online loan application, and everything browsed in-between.... Coremetrics Online Analytics provides the most accurate and complete record of visitor behavior—capturing every click of every visitor over time, and storing them in Coremetrics' LIVE (Lifetime Individual Visitor Experience) Profiles secure database. As a result, marketers can build a comprehensive and accurate record of online visitor behavior—a record that connects visitor behavior over time, so they can see all the marketing interactions each visitor has with the company."[51]

Social Media Marketing and "Digital Footprints"

Over the last few years, the growth of social networks has been accompanied by the development of a social media-marketing field. Social networks have now taken behavioral targeting to another level, allowing marketers to commercially target users based both on their online activities and self-disclosed profile information. Few social media users understand the wide range of data tracking and targeting that operates on and via these networks. Our communications on blogs, social networks and other Web 2.0 media are now being analyzed, including for the purpose of targeting what are called key or "Alpha" influencers (people whose opinion sways their network of relationships). As the authors of one recent book on the social media marketing industry explained, "The digitally networked visitor to

---

[49] x+1, "Our Technology," http://www.xplusone.com/solutions/technology.html (viewed 14 June 2009).

[50] Interwoven, "Autonomy Optimost Adaptive Targeting," http://www.interwoven.com/components/pagenext.jsp?topic=SOLUTION::ADAPTIVE_TARGETING (viewed 14 June 2009).

[51] Coremetrics, "Optimizing Marketing Spend of Financial Services: Leveraging Analytics in Marketing Budget Allocation."

these social media forms leaves behind footprints, shadows and trails of his or her individual collective endeavours in the form of data; data that enables new type of marketing and communication between and within consumer communications.... Over time, this process will lead to an understanding of the participant's digital footprint."[52] Products such as Nielsen's Buzzmetrics, BuzzLogic ("conversation ad targeting"), Ripple6 and Radian6 are part of this new digital data collection apparatus.[53]

So-called third-party applications, including small pieces of software known as widgets, "phone home" information about their users, contributing to industry's data collection practices. For example, RockYou, which has created popular applications available on Facebook and other sites, recently launched its "Social Video Ads and Cross Platform Video Distribution" service. The data it collects with video, it says, "go far beyond impressions. Audience interactions (views, stops, rewinds, sharing) are gauged by the millisecond and response can be measured, in real numbers. Advertisers who can combine that data with behavioral or demographic profiling, to reach exact targets, get amazing results."[54] Another company, Clearspring (which makes many popular widgets), explains that it provides "detailed real-time analytics... to understand where visitors are viewing your widget, where it is spreading from and how people are interacting with it."[55] Kontagent is a "Facebook-funded Partner" that can deliver an "accurate understanding of the demographics of a site's users, how the users are socially linked, and what social interactions occur among the site's users."[56] It can "track"

---

[52] Ajut Jaokar, Brian Jacobs, Alan Moore and Jouko Ahvenainen, *Social Media Marketing: How Data Analytics Helps to Monetize the User Base in Telecoms, Social Networks, Media and Advertising in a Converged Ecosystem* (London: Futuretext, 2009), pp. 2, 19.

[53] See, for example, Radian6, "Social Media Monitoring and Engagement for Agencies and the Enterprise," http://www.radian6.com/cms/solution; BuzzLogic, "Get Your Ads in Front of Passionate Consumers," http://www.buzzlogic.com/advertisers/conversation-targeting.html; Nielsen Online, "Millions of Consumer are Talking—Are You Listening," http://www.nielsen-online.com/products.jsp?section=pro_buzz; Ripple6, "Revolutionizing Research Through Online Conversations," http://www.ripple6.com/platform/socialInsights.aspx; Suresh Vittal, "The Forrester Wave: Listening Platforms, Q1 2009," 23 Jan. 2009, http://www.nielsen-online.com/emc/0901_forrester/The%20Forrester%20Wave%20Listening%20Platforms%20Q1.pdf. The Interactive Advertising Bureau recently published "Social Advertising Best Practices," http://www.iab.net/media/file/Social-Advertising-Best-Practices-0509.pdf (all viewed 14 June. 2009), which discusses some of data capture that occurs within social media, and ways of informing users.

[54] "RockYou Adds Video to its Ad Network," 3 Feb. 2009, http://blog.rockyouads.com/?cat=20 (viewed 15 June 2009).

[55] Clearspring, "Documentation: Reporting," http://www.clearspring.com/docs/reporting (viewed 15 June 2009).

[56] Kontagent, "Social Network Developers Demand New Class of Viral Analytic Tools," press release, 23 July 2008, http://www.kontagent.com/about/press/social-network-developers-demand-new-class-of-viral-analytic-tools/ (viewed 15 June 2009).

such data points as age, gender, location, number of friends, page views, and unique visits. Kontagent also tracks and measures what it calls the "virality" factor of a social networking application (such as a game), including "invite sent per user" and "invite and notification conversion rates" (meaning how a person responded to the invitation to download an application).[57]

Behavioral targeting is also being used in social networks. For example, Lotame's "behavioral targeting technology... analyzes behavior from consumers who chat-up brands on social media and community platforms...."[58] Its "Crowd Control" product "optimizes behavioral targeting by capturing previously unavailable data based on engagement, which is inherent to social media."[59]

As MySpace explained in 2008 to advertisers, its "HyperTargeting" system allows it to meld registration data ("personal demographic information provided by MySpace users when they become members") with MySpace Profile Data ("freely expressed information by consumers about their passions and interests"). The result, claims MySpace, is "Next-Generation Targeting."[60] Nor are MySpace users aware that their data are sent off to a data warehouse each day to be analyzed for "deep insights," including "real-time analysis to drive [Fox Interactive Media's] advanced targeted advertising systems."[61] Such data mining is increasingly part of the structure of the online ad-targeting universe.

Facebook, as you know, has had several well-publicized incidents involving its collection and use of data. After one recent flare-up, Facebook developed a set of "principles" and a "Statement of Rights and Responsibilities" that involved a discussion and a vote by its users.[62] But we believe that Facebook (and many other

---

[57] Kontagent, "The Kontagent Fact Sheet," http://www.kontagent.com/about/ (viewed 15 June 2009).

[58] Laurie Sullivan, "Lotame's Three-Way BT Deal Measures Attitude, Buzz," *Online Media Daily*, 2 Feb. 2009, http://www.mediapost.com/publications/?fa=Articles.showArticle&art_aid=99440 (viewed 15 June 2009).

[59] "Lotame Receives Multi-Million Dollar Series a Financing in a Round Led by Battery Ventures," press release, 11 Feb. 2008, http://www.reuters.com/article/pressRelease/idUS107393+11-Feb-2008+PRN20080211 (viewed 15 June 2009).

[60] MySpace Media Kit, 2008, personal copy.

[61] Aster, "MySpace.com Scales Analytics for All of Their Friends," 2009, www.asterdata.com/resources/downloads/casestudies/myspace_aster.pdf; "Data Warehouse Appliance from Sun and Greenplum Powers Hypertargeting for Fox/MySpace," Greenplum, 24 Sept. 2008, http://www.greenplum.com/news/106/231/Data-Warehouse-Appliance-from-Sun-and-Greenplum-Powers-Hypertargeting-for-Fox-MySpace/d,blog/ (both viewed 14 June 2009).

[62] Facebook, "Facebook Principles," 15 April 2009, http://www.facebook.com/note.php?note_id=183540865300; Rochelle Garner, "Facebook Creates Site Principles After Users Complain," *Bloomberg.com*, 26 Feb. 2009, http://www.bloomberg.com/apps/news?pid=20601103&sid=azLmshQcmBJw&refer=us (both viewed 15 June 2009).

social networks and related sites), fail to adequately tell its users about how their data is collected and used. For example, Facebook tells brand advertisers that they can take advantage of a user's profile: "A profile is any individual's online representation of self. Through their profiles, people share details about their interests, activities and even contact information.... Reach the exact audience you want with Facebook targeting. The Facebook targeting spectrum ranges from broad reach demographic and geographic preferences like networks and colleges to more granular and specific profile interests." An examination of Facebook's media kit—or any similar description by competitors—will reveal a system based on a digitally driven "viral" marketing approach. We believe this system is non-transparent and largely unaccountable to the majority of users.[63]

Much has also been said about what is claimed to be the self-correcting nature related to data collection practices and digital media, such as with Facebook. But although users did protest recently over Facebook's Terms of Service, it was the crucial role of consumer groups and the threat of regulatory action that actually brought the problem to light and forced the company to reconsider its practices. It was *The Consumerist*, owned by Consumers Union, that played the major role in identifying Facebook's proposed changes, which were influenced as well by a pending complaint that was going to be filed at the FTC by the Electronic Privacy Information Center and other privacy groups.[64]

Online Ad Exchanges: Data Bought and Sold in "12 milliseconds"

The monetization of our data and online behaviors is now being bought and sold in marketplaces that have so far been operating without the scrutiny of regulators or Congress. As *BusinessWeek* explained, "[A]d exchanges are sort of like stock exchanges for online ads. Web sites put ad space up for auction, and ad agencies, armed with demographic and behavioral data about the people who visit those sites, bid to place ads for their clients' campaigns."[65] Google, Yahoo, Microsoft, and others run such exchanges. Microsoft's AdECN ad exchange describes its process: "Advertisers... specify in advance the targeting they want, and how much they are willing to pay when such an opportunity comes up. That's their bid. The action

---

[63] Facebook, "Media Kit for Brand Advertisers," personal copy.

[64] Chris Walters, "Facebook's New Terms Of Service: 'We Can Do Anything We Want With Your Content. Forever,'" *The Consumerist*, 15 Feb. 2009, http://consumerist.com/5150175/facebooks-new-terms-of-service-we-can-do-anything-we-want-with-your-content-forever; Douglas MacMillan, "The Complaint Almost Filed Against Facebook," *BusinessWeek*, 18 Feb. 2009, http://www.businessweek.com/the_thread/techbeat/archives/2009/02/the_complaint_a.html (both viewed 15 June 2009).

[65] Robert D. Hof, "Google's Grab for the Display Ad Market," *BusinessWeek*, 11 June 2009, http://www.businessweek.com/magazine/content/09_25/b4136052151611.htm?campaign_id=rss_daily (viewed 15 June 2009).

starts when a viewer lands on a website page. That triggers a single-pass auction among all of the interested advertisers. In about 12 milliseconds—as the page is loading—we run the auction, the highest bidder wins, and we show that ad.... The advertiser knows that his ad is going to be shown on a page or a site with certain content, or at a certain time, or to a person with a certain profile, and so on.... We also offer behavioral, including a viewer's recent search queries, and profile-based targeting: age, gender, income.... We cull [profile data] through relationships with our partners. Here's how it works: when a viewer lands on a webpage in the exchange, we can tell if that viewer is known by one of our partners. If so, we query the partner, who tells us about that person...."[66]

The Growing Use of Neuroscience in Designing and Deploying Online Ads

Advertisers are increasingly using a range of what are called "neuromarketing" techniques designed to shape and help deliver marketing messages, including for the digital market. As part of the ad industry's "engagement" initiative, marketers, as one leading online marketing executive explained, are exploring how to harness the "subtle, subconscious process in which consumers begin to combine the ad's messages with their own associations, symbols and metaphors to make the brand more personally relevant."[67] Marketers are using such techniques as functional magnetic resonance imaging (fMRI), eye-tracking studies, galvanic skin response, and electroencephalology (EEG) to finely hone their strategies for digital advertising. Among the online marketing companies using some form of neuromarketing are Google, Microsoft, and Yahoo. Google used neuromarketing researcher NeuroFocus last year to test so-called "inVideo Ads" for its YouTube service. The study "used biometric measures such as brainwave activity, eye-tracking and skin response to gauge the impact of ads."[68] MTV recently "conducted a three-day study of more than 60 gamers at a biometrics lab in Las Vegas; they showed the players various ads and games, all while examining stats like heart rate, respiration, movement patterns and visual attention.... [T]hey found that 15-second pre-rolls were the most effective way to garner a player's 'focused attention.'"[69] The

---

[66] AdECN, "FAQ: The Auction," http://www.adecn.com/faq_3.html; AdECN, "FAQ: Targeting," http://www.adecn.com/faq_4.html (both viewed 15 June 2009).

[67] Jim Nail, "The 4 Types of Engagement," *iMedia Connection*, 13 Oct. 2006, http://www.imediaconnection.com/content/11633.asp (viewed 15 June 2009).

[68] Mike Shields, "Google, MediaVest Tap Biometrics for InVideo Ads Play," *Mediaweek*, 23 Oct. 2008, http://www.neurofocus.com/pdfs/neurofocus_google_taps_biometrics.pdf; Mark Walsh, "Google: This Is Your Brain On Advertising," *Online Media Daily*, 23 Oct. 2008, http://www.mediapost.com/publications/?fa=Articles.showArticle&art_aid=93319 (both viewed 15 June 2009).

[69] Laurie Sullivan, "BT: Can It Mean Behavioral Responses To Ads?" *Behavioral Insider*, 4 June 2009, http://www.mediapost.com/publications/?fa=Articles.showArticle&art_aid=107346; David Kaplan, "Need To Reach Casual Gamers? MTV Says 15-Second Pre-Rolls Work Best," paidContent.org, 10 June

ad industry's highest research award—the Grand Ogilvy—was awarded this year to a campaign for Frito-Lays Cheetos, with major online components that used an array of neuromarketing techniques.[70]

Behavioral Targeting and Mobile Marketing

Many of the same consumer data collection, profiling, and behavioral targeting techniques that raise concern in the more "traditional" online world have been purposefully brought into the mobile phone marketplace. Mobile marketers in the U.S. are already deploying a dizzying array of targeted marketing applications, involving so-called rich media, mobile video, branded portals, integrated avatars that offer "viral marketing" opportunities, interactive and "personalized wallpapers," "direct-response" micro-sites, and a variety of social media tracking and data analysis tools. Behavioral targeting is swiftly migrating to the mobile world. Mobile devices, which know our location and other intimate details of our lives, are being turned into portable behavioral tracking and targeting tools that consumers unwittingly take with them wherever they go. Enpocket, a leader in "intelligent mobile marketing" that was recently purchased by Nokia, provides a sobering example of the potential of this medium for behavioral targeting. Enpocket has developed a "Personalization Engine," which it described as "a system of analytical models that scores mobile users based on their past behavior. It enables us to predict which products and services a customer might purchase next. That way, we can provide the right message, advertisement or promotion to the right person at the right time. It can also forecast events, such as customer churn and will recommend effective customer engagements to preempt attrition. When integrated with the Marketing Engine, the result is highly relevant marketing messages, personalized recommendations, less churn, and higher sales of mobile consumables."[71]

U.S. consumers will, as you know, increasingly rely on their mobile devices for a wide range of services, including sensitive transactions related to finance and

---

2009, http://www.paidcontent.org/entry/419-mtvn-looks-to-biometrics-to-guide-casual-game-ads/#extended (both viewed 15 June 2009).

[70] Advertising Research Foundation, "The ARF 2009 David Ogilvy Awards," http://www.thearf.org/assets/ogilvy-09; "Grand Ogilvy Winner: 'Mischievous Fun with Cheetos,'" http://thearf-org-aux-assets.s3.amazonaws.com/ogilvy/cs/Ogilvy-09-CS-Cheetos.pdf. For more on the use of neuroscience and marketing, see Advertising Research Foundation Engagement Council, http://www.thearf.org/assets/engagement-council; Neurofocus (now partly owned by Nielsen), http://www.neurofocus.com/; Innerscope Research, http://www.innerscoperesearch.com/; and Olson Zaltman Associates, http://www.olsonzaltman.com/ (all viewed 15 June 2009).

[71] Enpocket, "Advanced Profiling and Targeting," http://www.enpocket.com/solutions/enpocket%20platform/advanced-profiling-and-targeting (viewed 1 July 2008).

health. We should not permit the expansion of behavioral targeting into the mobile world (where it will be combined with precise location information and history).[72]

Digital Marketing, Behavioral Targeting and Health

Consumers increasingly rely on the Internet and other online media for health advice and services. The Web, we recognize, is an important source for such information. But consumers seeking health information must be assured of the highest level of privacy protection. Pharmaceutical companies are now using digital marketing services—including what's called "unbranded" social networks.[73] There are also a growing number of health-related websites offering interactive advertising opportunities for marketers, including "condition-targeted" placement (facilitated by "widgets and viral elements"). Online ad giants, such as Time Warner's Platform A, have made presentations on "Behavioral Targeting for Pharmaceutical Marketers." The role of online data collection, interactive marketing, and its impact on the public health requires serious scrutiny from this committee, other lawmakers, and regulators.[74]

Digital Media and Marketing Data Consolidation

The online advertising business has witnessed dramatic consolidation over the last several years; major interactive giants have swallowed leading behavioral targeting and other data targeting companies. Google now operates DoubleClick; Yahoo acquired Blue Lithium and Right Media; Microsoft bought aQuantive and Screen Tonic; Time Warner's AOL acquired Tacoda and Third Screen Media; WPP took over 24/7 Real Media. As you know, last year there was a flurry of activity related to the future of Yahoo involving Microsoft and Google. A tiny handful of companies engaged in data collection that track, profile, and target us across websites, mobile applications, online games, virtual worlds, and search engines are playing an

---

[72] For a review of the state of mobile marketing, behavioral targeting and related concerns, see Center for Digital Democracy and U.S. PIRG, "Complaint and Request for Inquiry and Injunctive Relief Concerning Unfair and Deceptive Mobile Marketing Practices," Federal Trade Commission Filing, 13 Jan. 2009, http://www.democraticmedia.org/current_projects/privacy/analysis/mobile_marketing (viewed 15 June 2009).

[73] For example, Digitas Health works with AstraZeneca, Pfizer, Lilly, Merck and others. Digitas Health, "Clients," http://www.digitashealth.com/#/work/clients/. Ogilvy Healthworld provides a range of direct to consumer marketing services, including online. Ogilvy Healthworld, "Direct to Consumer, Direct to Client," http://www.ogilvyhealthworld.com/2-5_healthworld_services_dtc.html (both viewed 15 June 2009).

[74] See, for example, Waterfront Media, "Advertise with Us," http://www.waterfrontmedia.com/advertise-with-wfm.aspx; Healthline, "2009 Media Kit," www.healthline.com/corporate/media/healthline_media_kit_2009.pdf; and Platform A/AOL, "Behavioral Targeting for Pharmaceutical Marketers," 2006, personal copy (all viewed 15 June 2009).

important role shaping the Internet's future. Given the tremendous data collection capabilities inherent in digital marketing, and the growing concentration of influence by a few, the need for legislative action to protect consumer privacy is clear.

Multicultural Targeting

Another area that deserves scrutiny is the online marketing services specifically focused on the country's diverse multicultural communities, including African Americans and Hispanics. The collection of data identifying users by what is assumed to be their ethnic interests raises concerns about profiling and its impact. While I fully support the growth of a robust online ad system that creates diverse ownership of online publishing services, the implications of ethnic and racial data collection practices must be reviewed (including the growing number of online ad services focused on the Spanish-speaking U.S. market).[75]

Children and Adolescents

Young people, especially adolescents, are at the virtual epicenter of the digital marketing system. They are the focus of a wide range of digital marketing techniques, including behavioral targeting. A coalition of children's health, educational and advocacy groups, including the American Academy of Child and Adolescent Psychiatry, the American Academy of Pediatrics, the American Psychological Association, Children Now, the Center for Digital Democracy, and several others, has asked the FTC to prohibit all behavioral targeting to young people under 18. To see the extent of this targeting system, all one has to do is review how food and beverage marketers have deployed a sophisticated array of digital advertising, including online games, virtual worlds, social networks, interactive video, and the like. This country faces a youth obesity epidemic, which is taking its toll on the health of our young people, and will contribute to increasing

---

[75] There are online marketing firms, including ad networks, focused on what's called the multicultural market. See, for example, AdGroups.com, which offers marketers the ability to segment using such variables as ethnicity, gender, location, age, income status, entertainment interest, blogs and "Hip Hop Culture." AdGroups.com, "Ad Network + Exchanges Guide," http://brandedcontent.adage.com/adnetworkguide09/network.php?id=4. Major online marketers also target these groups. See, for example, Time Warner/AOL's Advertising.com "MediaGlow" online ad targeting network, which reaches "96.5% of Hispanics online," http://www.mediaglow.com/. Platform A explains that older Hispanic women are natural "viral marketers," able to influence purchases for food, music and video games. AOL Platform A, "Meet Carmen," http://www.platform-a.com/advertiser-solutions/audience-targeting/consumer-profiles/carmen-age-49 (all viewed 15 June 2009).

health costs. We respectfully urge the subcommittees to hold a separate hearing on privacy threats for both children and adolescents.[76]

Deep Packet Inspection and Behavioral Targeting

All of the data collection and targeted online marketing practices we describe in this testimony become even more grave when a network operator is permitted to engage in deep packet inspection. Given actions by the FCC, consumers must rely on a handful of cable and telephone networks for their broadband service. Deep packet inspection (DPI) technologies enable these network providers to track their subscribers' actions online (data that can then be merged with extensive customer information files). When the power of online ad profiling and targeting technologies are combined with the microscopic tracking and analysis capabilities of DPI, consumer privacy is further threatened.

The Failure of Self-Regulation

The practices we describe here, which are just the proverbial tip of the data-collection iceberg, have all emerged while the online ad industry was engaged in various forms of "self-regulation." Until the series of FTC complaints brought by CDD/USPIRG and others, and most notably until the political pressure brought upon that agency for its failure to address privacy concerns when it approved the Google/DoubleClick merger, the online ad industry's self-regulatory system was in a Rip Van Winkle-like deep slumber. It was only after the growing call for regulatory action, including from your subcommittees, that some in the online marketing industry finally admitted that privacy is an issue.[77] While there have been some promising developments in terms of reduced data retention and new forms of opt-in and opt-out procedures, they are the result of regulatory pressure—especially from the European Union's Article 29 Working Party. U.S. consumers should not have to

---

[76] Comments of American Academy of Child and Adolescent Psychiatry, the American Academy of Pediatrics, the American Psychological Association, Benton Foundation, Campaign for a Commercial Free Childhood, Center for Digital democracy, Children Now, and the Office of Communications of the United Church of Christ. Online Behavioral Advertising Principles, Federal Trade Commission, 11 April 2009, http://www.democraticmedia.org/news_room/letters/Letter_re_behavioral_advertising_comments; Kathryn C. Montgomery and Jeff Chester, "Interactive Food and Beverage Marketing: Targeting Adolescents in the Digital Age," *Journal of Adolescent Health*, 2009 (in press). For a good overview of contemporary digital marketing practices targeted at youth for fast foods and other high fat products, see "Digital Marketing Update," http://www.digitalads.org/updates.php (all viewed 15 June 2009).

[77] For an excellent critique about the failure of the Network Advertising Initiative, see Pam Dixon, "The Network Advertising Initiative: Failing at Consumer Protection and at Self-Regulation," World Privacy Forum, 2 Nov. 2007, http://www.worldprivacyforum.org/behavioral_advertising.html (viewed 15 June 2009).

rely on EU-based regulatory bodies to protect their privacy. Nor should we be content with piecemeal and incremental changes in policies due to the building pressure for real legislative and regulatory reform.[78]

Blessed by an antiquated federal policy that narrowly defines personal information as name, street address, or social security number, marketers claim that they don't violate our privacy because they may not have such information. But in today's online world, it isn't necessary to know someone's actual name or street address to actually identify—via cookies, IP addresses, and other online targeting techniques—how a particular person interacts online. We are glad the FTC has recently awoken to the realities of today's online marketplace, and has acknowledged that it must address this important issue.[79]

Privacy policies are an inadequate mechanism that fail to protect the public. As documented in a recent UC Berkeley School of Information study on online privacy, privacy policies are difficult to read; the amount of time required to read them is too great; they lead consumers to falsely believe their privacy is protected; there isn't meaningful differences between policies, leaving consumers with no alternatives; and consumers aren't really aware of the "potential dangers."[80]

I recognize that Google, Yahoo, and Microsoft, among others, have made some promising changes in their data collection practices. Google, for example, has developed a form of opt-in for its version of behavioral targeting—which it calls "interest-based." Google is initially creating segments for targeting, according to press reports, "across 20 categories and 600 subcategories" (and the company has reportedly promised that it won't target a number of sensitive areas, such as race, religion, sexual orientation "or certain types of financial or health concerns"). This move by Google, of course, comes after it incorporated behavioral targeting technology leader DoubleClick into its holdings. Google will be offering such behavioral targeting across both its "text ads and display network." Given Google's other targeting capabilities, including on YouTube, we strongly believe that even this new system will fail to adequately inform consumers about the extent of their

---

[78] "Federal Trade Commission Closes Google/DoubleClick Investigation," press release, 20 Dec. 2007, http://www.ftc.gov/opa/2007/12/googledc.shtm. The dissent from FTC Commissioner Pamela Harbour and pressure from privacy and consumer groups helped force the agency to issue proposed self-regulatory privacy principles on the same day it approved the merger. The EU's Article 29 Working Party, and generally the stronger safeguards on data protection in the EU, has forced major online companies to alter some practices to better protection privacy. See European Commission, Justice and Home Affairs, Data Protection Working Party, "Online Consultations," http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/consultations/index_en.htm (both viewed 15 June 2009).

[79] "FTC Staff Revises Online Behavioral Advertising Principles," press release, 12 Feb. 2009, http://www.ftc.gov/opa/2009/02/behavad.shtm (viewed 15 June 2009).

[80] Joshua Gomez, Travis Pinnick, and Ashkan Soltani, "KnowPrivacy,"1 June 2009, http://www.knowprivacy.org/ (viewed 15 June 2009).

data collection and its impact on their privacy. Nor should consumers be willing to accept promises that a company will not target based on past search queries or so-called "sensitive data, since such policies could change over time.[81]

The Role of the FTC

The FTC has been largely incapable of ensuring American privacy is protected online. Staff has been reined in from more aggressively pursuing the issue, primarily to ensure that industry self-regulation remains as the agency's principle approach. The FTC is also encumbered with a lack of staff working on privacy and online marketing issues, including personnel familiar with the technical characteristics of contemporary marketing. As we mentioned earlier, its recent adoption of self-regulatory principles was made possible only because of the political controversy generated by a merger review. The FTC needs to have additional resources, especially so it can better protect consumers from digital marketing transactions involving their financial and health data. Congress should press the FTC to be more proactive in this arena.

We are confident that the FTC is now ready to address online marketing and consumer privacy more meaningfully than in the past. Chairman Jon Leibowitz has already stated he wants to see real progress on the issue. His appointment of highly regarded legal scholar and consumer advocate David Vladeck as the new director of the Bureau of Consumer Protection is a positive sign that the FTC will now take digital marketing issues very seriously.

The Role of Congress

We urge you to enact legislation that would ensure that consumer privacy online is protected. The foundation for a new law should be implementing Fair Information

---

[81] Elyse Tager, "Behavioral Targeting Takeaways From ad:tech SF," *Clickz*, 13 May 2009, http://www.clickz.com/3633682; Barry Schwartz, "Google Gets Into Behavioral Targeting, Launches 'Interest-Based Advertising' Beta," Search Engine Land, 11 May 2009, http://searchengineland.com/google-introduces-interest-based-advertising-beta-16855. How such a system can be changed over time to permit greater targeting is illustrated by an exchange Schwartz had with a Google executive: "I asked Google how detailed can these ads get? I asked, can an advertiser pass along a specific ad to a specific user? For example, can I show an ad for the Sony HDR-XR200V if this user added the Sony HDR-XR200V to their shopping cart on my site but did not check out? Bender said yes, but ultimately it is up to the advertiser how specific they want to get with those ads." In the same article search expert Danny Sullivan added that Google had confirmed it had "tested behaviorial targeted ads using past search history data." Google executives had initially expressed some reservations about engaging in behavioral targeting. Eric Auchard, "Google Wary of Behavioral Targeting in Online Ads," *Reuters*, 31 July 2007, http://www.reuters.com/article/technologyNews/idUSN3135052620070801 (all viewed 15 June 2009).

Practices for the digital marketing environment. Notice and Choice, which has been the foundation of the self-regulatory regime, is a failure. Despite self-regulation, what we have witnessed is increasing data collection and use—all without the real, informed understanding and consent of users. Americans shouldn't have to trade away their privacy and accept online profiling and tracking as the price they must pay in order to access the Internet and other digital media. The failure to adequately regulate the financial sector greatly contributed to the worst economic crisis since the Great Depression. Regulation isn't a dirty word. It's essential so consumers and businesses can conduct their transactions with assurance that the system is as honest and accountable as possible.

The uncertainty over the loss of privacy and other consumer harms will continue to undermine confidence in the online advertising business. That's why the online ad industry will actually greatly benefit from privacy regulation. Given a new regulatory regime protecting privacy, industry leaders and entrepreneurs will develop new forms of marketing services where data collection and profiling are done in an above-board, consumer-friendly fashion. Consumer and privacy groups pledge to work closely with the subcommittees to help draft a law that balances the protection of consumers with the interests of the online marketing industry.

Mr. RUSH. Thank you, Mr. Chester. Now the chair recognizes Mr. Curran for 5 minutes.

TESTIMONY OF CHARLES D. CURRAN

Mr. CURRAN. Thank you, Chairman Rush, Chairman Boucher, and members of the subcommittee. I would like to thank you on behalf of the Network Advertising Initiative for the opportunity to discuss both the economic benefits and the privacy obligations of online behavioral advertising. The NAI is a coalition of advertising networks and other online marketing companies dedicated to responsible business practices and effective self-regulation. Originally founded 9 years ago, the NAI has grown to include more than 30 leading online advertising companies including all 10 of the largest advertising networks. Today, through the NAI's Web site consumers can learn more about or opt out of online behavioral advertising by any or all of the NAI's member companies across the many thousands of web sites on which such advertising is served. Today's hearing focuses on both industry practice and consumer expectations.

The NAI and its members are committed to online advertising practices that strike the right balance between consumers' economic and privacy expectations. We believe that consumers enjoy the diverse range of web sites and services that they get for free thanks to relevant advertising, but we must also provide consumers with meaningful notice and choice. Tens of millions of Americans benefit every day from free web content and services made available on the web because of banner advertising served by NAI members. These ad-supported services include news, blogs, video, photo sharing, and social networking services. NAI members support these web sites by connecting them with advertisers and by using web browser cookies to serve their visitors with more relevant and compelling advertisements.

NAI members provide web sites with a broad variety of services. They help smaller web sites combine their audiences so they can attract larger advertisers. They help advertisers gauge the success of their campaigns across multiple sites, and they also make online advertising more interesting and useful to consumers by using nonpersonally identifiable information about users' activity within an ad network to try to predict their likely interests. In the early days of online behavioral advertising more than 10 years ago, advocates and regulators challenged industry to provide appropriate privacy protections around browser cookies. The NAI self-regulatory code was established to meet that challenge and continues today to apply the same core principles for our members. First, users should receive clear and conspicuous notice on the web sites that they visit where data is collected and used.

Second, users should have the ability to opt out of behavioral advertising. Third, sensitive data should not be used for online behavioral advertising without a user's affirmative consent. Fourth, a user's affirmative consent should also be obtained if personally identifiable information is merged with information previously gathered about the user's web browsing with an ad network. As these technologies have matured and the online marketplace has diversified, the Federal Trade Commission has called on industry

to broaden and enhance its approach to self-regulation. The NAI and its member companies believe that self-regulatory approaches should be as dynamic as the online marketplace that they serve, and we are moving quickly to respond.

The NAI member companies are working to develop technologies that would support and enhance consumer notice in or around behaviorally based banner ads. This would allow users to learn more about behavioral advertising and to make choices directly from the ad itself. Additionally, to help protect users' choices, the NAI is implementing technology to improve the durability of user opt out preferences stored in browser cookies. The NAI believes that its current opt out approach strikes the right balance and consumers' expectations for today's cookie-based advertising. The model combines an opt out for the use of non-sensitive, non-personally identifiable information to deliver ads with an opt in requirement for use of sensitive or personally identifiable data. This preserves a default experience in which web sites provide users with more rather than less relevant advertising.

Users have multiple options to control behavioral advertising either by using opt outs offered by the NAI's members or their own easily accessible web browser tools. Any significant changes to this model such as requiring a user's opt in even to non-personally identifiable uses of cookies to improve the relevance could pose a profound risk to both the user's experience and the economic model for ad-supported web services. As they navigate from site to site, consumers could be inundated with recurring opt in prompts asking their permission to serve relevant ads. Consumer rejection of this approach could uproot the revenue model that supports many web sites today. It is vital to the continued growth of web services that the right balance is struck between the economic, technological, and consumer protection considerations relating to online advertising. The NAI looks forward to working with the subcommittees as they consider these important online privacy issues. Thank you.

[The prepared statement of Mr. Curran follows:]

Statement of Charles Curran
Executive Director, Network Advertising Initiative

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

Behavioral Advertising:
Industry Practices and Consumers' Expectations
June 18, 2009

Chairman Rush, Chairman Boucher and Members of the Subcommittees: The Network Advertising Initiative ("NAI") appreciates the opportunity to testify about online advertising generally and behaviorally-related advertising in particular. The NAI is a coalition of leading online advertising companies committed to developing actionable self-regulatory standards that establish and reward responsible business and data management practices and standards. The NAI maintains a centralized choice mechanism that allows consumers to opt out of online behavioral advertising by some or all of the NAI's member companies, across the many different Web sites on which NAI members provide such targeting (via www.networkadvertising.org).

The NAI's testimony today will focus on the business models and technologies deployed by its members to enhance the relevancy of online advertising, including behavioral advertising; the economic benefits to Web content providers and consumers that result from these advertising technologies; and the steps taken by NAI members to enhance corresponding consumer confidence through a self-regulatory Code of Conduct designed to promote transparency and choice for online behavioral advertising.

I. The Role of NAI Member Advertising Technologies in the Internet Marketplace, and their Economic Benefits

The Network Advertising Initiative's members include significant online advertising companies such as AOL's Platform-A division, Akamai, Microsoft's aQuantive division, Google, Yahoo!, AlmondNet, Audience Science, BlueKai, Media6Degrees, SpecificMEDIA and 24/7 Real Media. The NAI's membership now incorporates not just the ten largest advertising networks, but also leading data exchange and marketing

analytics services providers.[1] The business models of the NAI's members are based on the common goal of enabling Web content and services providers to enhance the relevancy (and efficiency) of their online display advertising, and to generate increased revenue to subsidize consumers' use of such services.

A. How NAI Members help Web content and services providers enhance their advertising revenue

Over the past 15 years, the World Wide Web has provided consumers access to an incredible variety of new services, ranging from online news, blogs, and other content to e-mail, search, social networking, video, and other Web-based services. The explosion in Web services and their ease-of-use have transformed consumers' ability to access public information and entertainment, and created entirely new platforms for community and collaboration. Web-based technologies have also radically enhanced the ability of small businesses and specialty content providers to establish and connect with new audiences, creating new jobs and substantially increasing the diversity of public discourse. Consumer consumption of such Web services has continued to grow rapidly.[2]

The great majority of these Web sites and services are currently provided to consumers free of charge. Instead of requiring visitors to register and pay a subscription fee, the operators of Web content and services subsidize their offerings with various types of advertising. These advertising revenues provide the creators of free Web content and services – site publishers, bloggers, and software developers – with the income they need to pay their staffs and build and expand their online offerings.

Display advertisements – sometimes called "banner" ads – are an important means by which many Web content and services providers (also called "Web publishers") generate such advertising revenue. For every Web page that is viewed by a user, the site or service has an opportunity to serve one or more display advertisements. Web publishers use ad serving technologies to manage this "inventory" of potential banner ad

[1] In the past year, the NAI's membership has nearly doubled in size, growing from 15 to 29 members, with an additional three companies (including ValueClick) implementing NAI membership. The ten largest advertising networks, as measured by audience reach, are NAI members. *See* comScore Media Metrix, *comScore Releases April 2009 U.S. Ranking of Top 25 Ad Networks, available at* http://ir.comscore.com/releasedetail.cfm?releaseid=385312.

[2] *See generally* Center for the Digital Future, USC Annenberg School for Communication, *Highlights from the 2009 Digital Future Report* (April 2009), *available at* http://www.digitalcenter.org/pdf/2009_Digital_Future_Project_Release_Highlights.pdf (noting that 51% of consumers prefer ad-supported online content); The Nielsen Company, *Television, Internet and Mobile Usage in the U.S. – A2 M2 Three Screen Report* (1st Quarter, May 2009), *available at* http://blog.nielsen.com/nielsenwire/wp-content/uploads/2009/05/nielsen_threescreenreport_q109.pdf (noting continued growth in monthly Internet usage generally by over 160 million U.S. users, and of online video in particular). Cisco expects Internet traffic to grow fivefold by 2013. *See* Cisco, *Cisco® Visual Networking Index (VNI) Forecast and Methodology, 2008-2013* (Summary, June 2009), *available at* http://newsroom.cisco.com/dlls/2009/prod_060909.html. *See also* IAB/Hamilton Consultants Inc., Drs. John Deighton and John Quelch, *Economic Value of the Advertising-Supported Internet Ecosystem* at 4 (June 10, 2009), *available at* http://www.iab.net/economicvalue (estimating that the advertising-supported Internet accounts for $300 billion of economic activity).

placements: the publisher must estimate the overall number of potential ad "impressions" that are available for different advertisers to purchase, and must then also deliver the advertiser's campaign and report on its effectiveness.

Display-related ads are a very significant source of income to Web content and services providers, generating approximately $7.6 billion in advertising revenue in 2008.[3] These Web publishers have a dual incentive to ensure that they serve their users with the most relevant banner ads possible: not only do more relevant advertisements generate greater user response and revenue for the publisher; greater ad relevance enhances the user experience and avoids the potential nuisance effect to users from less customized marketing.[4]

Web publishers have a variety of potential approaches to ensuring such relevance. The most direct approach is to match the subject matter of banner advertisements to the content or subject matter of the page on which it is displayed: for example, an ad for ocean cruise on a Web page devoted to Caribbean travel. However, such "contextually" targeted advertisements are not always feasible for every type of Web content: for example, an online photo sharing service, or an online newspaper's section devoted to international affairs coverage, are not as readily suited to contextual advertisements. Web publishers must rely on other potential attributes of their Web site visitors to help ensure ad relevance, such as registration information reflecting their gender, age, or zip code; or, alternatively, other potential interests of their users inferred from prior Web activity, either on the publisher's site or elsewhere on the Web. And even for large Web sites or services providers, there is no assurance that they will be able to sell their entire potential advertising inventory at rates sufficient to support their operating costs.

Smaller-scale Web publishers – such as blogs and specialty interest content sites – face an additional challenge. The monthly audiences of these sites vary in size from hundreds of thousands to millions of visitors.[5] Such small Web publishers cannot employ their own dedicated sales force to sell their banner inventory to potential advertisers. More

---

[3] *See* Interactive Advertising Bureau, *2008 IAB/PricewaterhouseCoopers Internet Advertising Revenue Report* (March 2009), *available at* http://www.iab.net/media/file/IAB_PwC_2008_full_year.pdf). The report notes that display-related advertising includes display banner ads (21% of 2008 full year revenues or $4.9 billion), rich media (7% or $1.6 billion), digital video (3% or $734 million), and sponsorship (2% or $387 million). *Id* at 9. Moreover, e-commerce providers separately provide a substantial amount of proprietary advertising, encouraging commerce. IAB/Hamilton Consultants Inc., Deighton and Quelch, *Economic Value of the Advertising-Supported Internet Ecosystem, supra* note 2 at 3.

[4] One TRUSTe study found that when online advertising for products and services is not relevant to consumers' wants and needs, 72% of consumers find the experience intrusive or annoying. *See* TRUSTe, *2008 Study: Consumer Attitudes about Behavioral Targeting* (March 28, 2008), *available at* http://www.truste.com/pdf/TRUSTe_TNS_2008_BT%20_Study_Summary.pdf.

[5] The statistical diversity of smaller Web sites outside the large-traffic Web sites is sometimes referred to as the Web's "Long Tail." *See, e.g.,* Interactive Advertising Bureau, *I Am the Long Tail* (2009) *available at* http://iamthelongtail.com/ (offering video examples of the extraordinary diversity in subject matter and business types of small Web publishers). *See also* Mark Penn, *America's Newest Profession: Bloggers for Hire*, Wall St. J. (April 21, 2009) (estimating that there are 20 million bloggers, with 1.7 million profiting from their work, and more than 450,000 using blogging as their primary source of income).

importantly, the smaller audiences of such sites do not easily lend themselves to the execution of large-scale brand advertising campaigns preferred by major companies.

The advertising networks, exchanges, and other business models represented in the NAI are vital partners for Web publishers – both large and small – in finding advertisers for their audiences, helping to enhance the relevance of the advertisements served to their users, and thereby generating the revenue needed for these publishers to serve consumers. The important functions NAI members provide include:

- Acting as intermediaries for Web publishers and advertisers, by acquiring unsold impressions from both large and smaller Web content sites, and aggregating them into potential audiences for advertisers (for example, generating a multi-site campaign for a movie's opening weekend);
- Supporting a variety of pricing models for advertisers, including cost-per-impression (CPM) pricing preferred by brand awareness advertisers; or cost-per-action or click (CPA or CPC) pricing favored by advertisings looking to generate direct online sales (for example, banner ads for online universities);
- Offering niche-based approaches for particular types of publishers (ad networks focused on auto or women's interest publisher sites); and
- Using online advertising technologies to aggregate insights from single or multiple Web publishers to enhance the relevance and quality of user advertisements

Over the past decade, NAI member companies have been at the forefront of technological innovation designed to bring more efficient and scalable approaches to online advertising, enhancing the potential revenue opportunities for both large and small Web publishers.

B. The use of cookie technology to help increase the relevancy of advertisements

NAI member companies primarily rely on Web browser (HTTP) cookies and similar technologies to manage their ad serving functions. HTTP cookies are small text files that are stored inside a user's browser, and that usually contain a random string of numbers intended to serve as a unique identifier for the user's browser.[6] Such cookies help address the problem that Web browsers cannot otherwise easily "remember" the same user from Web page to Web page, and are employed for a variety of purposes other than advertising. For example, cookies allow a browser to continue to recognize a user across multiple Web pages; to maintain authentication; and to maintain an online shopping cart.

In the advertising context, HTTP cookies help advertising networks to remember an individual user's browser over time and to make decisions about which ad may be most relevant to serve back to that user. Among other things, cookies enable advertising networks to carry out the following functions:

[6] *See, e.g.*, Wikipedia, HTTP cookie, *available at* http://en.wikipedia.org/wiki/Http_cookie (last accessed June 15, 2009).

- Limiting the number of times a user sees the same ad, or serving ads in particular sequence;
- Determining on an aggregate basis how well particular ads perform to broad audiences (and adjusting ad delivery to serve fewer of unpopular ads);
- Allowing a user who visited a particular Web site to subsequently receive an ad related to that Web site while visiting a different site (e.g., a visitor who shops for prices at an online travel site receives an air fare promotion banner ad the next day when visiting their online mail box);
- Improving ad relevancy through behavioral information gathered over time and across multiple Web sites in order predict a user's possible interests (e.g. that a user visits many sport-related sites and is therefore likely to be interested in sports-related advertisements); or
- Remembering a user's opt-out preference for behaviorally-related advertising, or any other user preference.

When a Web publisher contracts with an advertising network to help serve ads on its Web site, it authorizes the ad network to serve ads from its own servers onto the Web publisher's site. It may also allow the ad network to place its cookies in the browser of visitors to the Web site. From the user perspective, cookies placed by advertising networks appear to have different Web domain addresses than the Web domain of the publisher (for example, a visitor to www.washingtonpost.com receiving a cookie from an ad network such as Advertising.com). If the domains are different than that of the Web site, browsers classify them as "third party" cookies (i.e. because the server for the advertising network's domain is located outside of the domain of the site which the user is visiting). A visitor to a particular Web site may still receive a variety of cookies served by the site operator (for example, a "first party" authentication cookie remembering that the user previously logged in to the site), as well as from third party advertising networks engaged by the Web site operator for ad serving purposes.

The placement of such advertising cookies on multiple partner Web sites creates the "network" of sites for which the ad network has the ability to recognize users: and that "network" is only as broad as the number of participating Web publisher sites that have chosen to allow the ad network to serve ads on their sites. Advertising networks vary considerably in scale and in the number of their partner Web sites: they do not have the ability to record information relating to the entirety of a user's Web browsing activity. The browser and HTTP cookie-based approach to online advertising is different from other technological approaches to online advertising, such as advertising targeting that relies on interactive software stored on the user's computer that can collect information about the totality of a user's Web behavior.[7]

An important feature of such third party cookies is their ability to allow ad networks to recognize users on a non-personally identifiable basis. A Web site visitor may, or may not, log in on the particular Web site that they visit. When an ad network serves a third

[7] The browser and cookie-related advertising model deployed by ad networks are also technologically distinct from advertising models that rely on Web browsing information derived through the user's Internet service connection.

party cookie on a user's browser with the Web site operator's permission, the site operator is not obliged to share information about the user's identity: indeed, for the ad network, the user's actual identity may be entirely unnecessary in order to carry out advertising-related functions. As a result, when information is gathered by an ad network over time using third party cookies, the ad network need not combine information about the user's actual identity with user interest or preference information that is associated with the unique identifier in the browser cookie.

Because cookie-related advertising technologies have been in use for well over a decade, Web browser software has evolved to provide users with robust control mechanisms. The major Web browsers offer users the ability to refuse to accept third party cookies of any type (including from ad networks), as well as to erase all third party cookies on request. Additionally, many security software products offer additional features allowing users to manage or limit third party cookies within their browsers.

C. The economic benefits of NAI Members' online advertising technologies

The advertising technologies deployed by NAI members provide considerable economic benefits across the entire online ecosystem, including for publishers, advertisers, and consumers.

From the Web publisher perspective, such advertising technologies enable and preserve their ability to operate their sites free of charge, without adopting subscription requirements (which would also significantly limit the size of their audience):

- Large Web sites derive incremental revenue for the sale of ad impressions that they themselves cannot sell, and that would otherwise generate no income;
- Smaller Web sites in particular -- for example, specialty interest sites or regional online newspapers -- can have their available advertising impressions aggregated into combined audiences attractive to larger-scale advertisers who may pay higher rates and thereby provide them the revenue they need to continue to operate; and
- Both types of Web sites gain access to online advertising technologies, such as re-targeting or behavioral advertising, that enable them to serve more relevant and profitable ads on portions of their sites that do not lend themselves to contextual advertising approaches.

From the perspective of advertisers, the principal benefits of these technologies lies in their adaptability to the challenges of an increasingly fragmented Web audience, as online usage continues to diversify across an ever-broader array of content and services:

- Through more relevant ads served to a more focused audience, the advertiser eliminates wasteful spending on irrelevant ads (for example, automotive advertisers can significantly reduce their advertising expenditures by serving ads for a new car model only to users who have actually expressed interest in that model by researching it, rather than blanketing a wider audience with such ads);

- Larger advertisers gain access to audiences that may be distributed across a great variety of small Web sites, and avoid the otherwise prohibitive costs of attempting to negotiate their ad campaigns on a site-by-site basis;
- Smaller-scale advertisers gain new opportunities to reach focused audiences online that would not have been available to them in the offline world;
- Technologies like re-targeting allow an advertiser to offer an improved price offer to a prior visitor to the advertiser's Web site;
- Behavioral advertising technologies result in a several fold increase in user response; [8] and
- Compared to other forms of advertising, online ads continue to offer far greater insight into the effectiveness of advertisers' spending, as well as greater flexibility for advertisers to pay only for ads that actually produce a result (performance-based ads that may be particularly important for industries with limited ad budgets).

Finally, from the perspective of the consumer, these online advertising technologies produce very significant economic (and non-economic) benefits:

- As previously discussed, the increased revenues associated with relevant advertising are vital to supporting the continued growth in free-of charge Web content and services (the business model for which consumers have expressed strong preference as compared to fee/subscription-based content and services);[9]
- The particular advantages of these advertising models for smaller Web publishers helps generate the revenue to sustain a greater diversity of content offerings and viewpoints;
- More relevant ads help reduce the potential nuisance effect of non-relevant advertising; and
- Ad-supported business models continue to remain the principal source of venture and investment capital for innovation in Web services that have enjoyed rapid consumer adoption (e.g., social networks).

II. The NAI's Self-Regulatory Approach to Consumer Transparency and Choice for Online Behavioral Advertising

Consumers' confidence in the online medium generally, and in online advertising specifically, is a critical component to the continued growth in Web content and services. It is also a clear prerequisite to the economic benefits of ad-supported business models

[8] The potential effectiveness of behaviorally targeted advertising is evident not only in the marketplace (where firms offering such technologies have achieved rapid growth); recent empirical research indicates a possible uplift of 670% in user click through rates when behavioral targeting segments are used. *See* Jun Yan, Gang Wang, Yun Jiang et. al., *How Much Can Behavioral Targeting Help Online Advertising?* at 261 *(WWW 2009 Madrid* April 20–24, 2009), *available at* http://www2009.eprints.org/27/1/p261.pdf.

[9] For example, in 2007 the New York Times abandoned an online-subscription based model in favor of an advertising-supported model available to all readers. *See* Richard Pérez-Pena, *Times to Stop Charging for Parts of Its Site,* N.Y. Times (Sept. 18, 2007), *available at* http://www.nytimes.com/2007/09/18/business/media/18times.html.

for publishers, advertisers and consumers alike. The NAI has a long-standing commitment to consumer notice and choice, among other fair information practices, as a means of promoting trust in the online advertising practices of its member companies.[10]

A. The NAI's introduction of privacy principles for third party advertising

The NAI was established in 2000 in response to concerns about advertising networks' use of HTTP cookies for the collection of Web browsing information for behaviorally-related ad serving, and the perceived lack of transparency and consumer choice mechanisms for this practice. In reviewing these practices, the Federal Trade Commission specifically criticized the sufficiency of Web publishers' disclosure of advertising networks' data collection practices, as well as the absence of a consumer choice mechanism to preclude the use of data gathered across a network of Web sites for advertising purposes.[11]

The NAI's founding companies[12] worked with the Federal Trade Commission to establish a principled self-regulatory framework that applied fair information practices to the complex business-to-business data collection and sharing practices between Web publishers and advertising networks. From the outset, the fundamental challenge in applying traditional fair information practice principles for personally-identifiable information – such as notice, choice, access and security – lay in the fact that the online behavioral advertising practices at issue involved non-personally identifiable information. Additionally, the goal of enhanced transparency to promote awareness of the advertising practices necessitated a new level of cooperation between Web publishers and their partner ad networks.

The NAI's 2000 Principles[13] chartered the following key self-regulatory principles for online behavioral advertising:

1. Notice: Recognizing that consumers overwhelmingly interact on the Web via consumer-facing websites, the NAI Principles required that notice about behavioral advertising practices must appear not only on NAI member

[10] Consumer awareness of third party advertising practices has increased over time. *See* TRUSTe, *supra note* 4 (noting that 71% are aware that their browsing information may be collected by a third party for advertising purposes). Consumer attitudes to online behavioral advertising remain, however, mixed. *Compare, e.g.,* Harris Interactive/Westin Survey, *How Online Users Feel About Behavioral Marketing and How Adoption of Privacy and Security Policies Could Affect Their Feelings* (March 27, 2008) (finding that a majority (55%) of consumers are comfortable with Web browsing data being used to serve customized ads when consumer privacy protections are put in place), with TRUSTe, *supra* note 4 (57% of consumers say they are not comfortable with advertisers using that browsing history to serve relevant ads, even when that information cannot be tied to their names or any other personal information).

[11] *See generally* Federal Trade Commission, *Online Profiling: A Report to Congress (Part 2, Recommendations)* (July 2000), *available at* http://www.ftc.gov/os/2000/07/onlineprofiling.htm.

[12] 24/7 Media, AdForce, AdKnowledge, Avenue A, Burst! Media, DoubleClick, Engage, and MatchLogic.

[13] *See* Network Advertising Initiative, *Self-Regulatory Principles for Online Preference Marketing by Network Advertisers* (2000), *available at* http://www.networkadvertising.org/pdfs/NAI_principles.pdf.

companies' own business websites, but also clearly and conspicuously on the Websites where data are collected and behaviorally-related advertising occurs. Notice would be implemented through contractual requirements for website partners that their privacy policies contain clear and conspicuous notices and a link to consumer choice about the practice of online behavioral advertising.[14]

2. Choice: The Principles mandated that notices provided to consumers include a consumer choice method commensurate with the type of data used for behavioral advertising:

   - Clear and conspicuous notice and opt-out choice (appearing in the publishers' privacy policy with a link to the network advertiser or an NAI opt-out Web page) would be required for use of non-personally identifiable information for online behavioral advertising;
   - On sites where multiple network advertising companies collect information (generally non-personally identifiable information), consumers would be able to opt out of behavioral advertising by any or all of the network advertisers on a single page accessible from the host Web site's privacy policy;
   - Additional protections would be required for any merger of personally identifiable information about consumers with non-personally identifiable information about Web activity separately gathered by ad networks for behavioral advertising purposes:
     - "Robust notice" and opt-out choice by the consumer (appearing at the time and place of information collection and before PII is entered) would be required for any merger occurring on a prospective basis;
     - Affirmative (opt-in) consent of the consumer would be required for any merger occurring retroactively for Web activity data already gathered by the ad network
   - Material changes in the information practices of a network advertising company could not be applied to information collected prior to the changes in the absence of affirmative (opt-in) consent of the consumer.

3. Other protections: Consistent with its goal of incorporating fair information practices, the 2000 NAI Principles prohibited the use of sensitive personally identifiable information (such as medical or financial data, sexual behavior or sexual orientation, or social security numbers) for online behavioral advertising. The Principles also required that if personally identifiable information was to be used for online behavioral advertising, additional protections relating to consumer access, reasonable security, and reliable sourcing should apply.

[14] *Id.* at Section II.D.1.

Commended by the FTC,[15] the 2000 NAI Principles were the first online advertising framework for self-regulation that explicitly addressed the online uses of non-personally identifiable data for advertising. Moreover, at a time when privacy policies had not universally been adopted by Web publishers as a consumer-facing tool, the NAI 2000 Principles' requirement that ad networks require such disclosure in their thousands of contracts served as an important driver to the widespread adoption of consumer-facing notice and opt-out link disclosures for online advertising. Most importantly, the voluntary adoption of these principles by ad networks in their capacity as business-to-business service providers – and the concurrent assumption of liability for deceptive practices – contributed substantially to the principle of online accountability for behavioral advertising.

B. The evolution of the NAI's self-regulatory initiatives for online advertising

Since 2000, the NAI and its member companies have continued to leverage their technological expertise by contributing to self-regulatory schemes that go beyond cookie-related online behavioral advertising. In 2003, the NAI established a division to represent legitimate email marketing companies working to fight the emerging threat of SPAM email practices, and to establish consensus-driven best practices for the email marketing industry.[16] In 2004, the NAI published guidelines for appropriate privacy, transparency and choice controls for use of web beacons (a pixel technology that can be used for data collection on Web pages to help enable online advertising collection and reporting).[17] In 2005, the NAI convened the "eCommerce in the Age of Spyware" forum, publishing papers from a broad spectrum of e-commerce companies, portals, network advertisers, behavioral marketers, anti-spyware vendors, and regulators.[18] These NAI-led policy efforts have contributed to the development of appropriate public policy responses to consumer concerns about online advertising technologies.

With the rapid growth and diversification of online advertising, coupled with related industry mergers and acquisitions, the FTC in 2007 convened a Town Hall Forum to revisit industry self-regulatory practices for online behavioral advertising.[19] In response to the FTC's ensuing staff proposals for behavioral advertising principles, the NAI and its

---

[15] *Online Profiling: A Report to Congress, supra* note 11 at Section III ("The Commission commends the NAI companies for the innovative aspects of their proposal and for their willingness to adopt and follow these self-regulatory principles.").

[16] Now an independent organization, the Email Sender & Provider Coalition (ESPC) currently represents 67 leading email marketing companies. *See generally* http://www.espcoalition.org.

[17] Network Advertising Initiative, *Web Beacons – NAI Guidelines for Notice and Choice, available at* http://networkadvertising.org/networks/Web_Beacons_rev_11-1-04.pdf.

[18] Network Advertising Initiative, *eCommerce in the Age of Spyware, available at* http://www.networkadvertising.org/spyware-forum/.

[19] *See* Comments by the Network Advertising Initiative for Federal Trade Commission Town Hall, *eHavioral Advertising: Tracking, Targeting and Technology* (November 2007), *available at* http://www.ftc.gov/os/comments/behavioraladvertising/071019nai.pdf.

members began a comprehensive process to revise its 2000 Principles. In April 2008, the NAI published for public comment a draft update to the Principles. Following this public comment period, the NAI in December 2008 issued its final updated Principles. [20]

The NAI's 2008 Self-Regulatory Code of Conduct contains the following key enhancements:

- The 2008 Self-Regulatory Code preserves the core commitment to transparency and choice for online behavioral advertising. NAI members must (a) require that web publishers clearly and conspicuously disclose NAI members' data collection and use practices; and (b) provide Web users with access to a consumer opt-out mechanism (through a conspicuous link to the opt out provided by the NAI member and/or a link to the NAI website consumer opt out).
- Although consumer notice through the privacy policies of Web sites remains the primary expected means for NAI members to comply with their notice requirement, the 2008 Self-Regulatory Code anticipates further enhancements to the technological underpinnings of the ad serving process that would allow for alternative means of consumer notice.[21]
- The 2008 Self-Regulatory Code retains the commitment to require consumer opt-in for the merger of personally identifiable information with non-personally identifiable data about their past Web browsing activity.
- Consumer opt-in is required for uses of sensitive information in connection with behavioral advertising. In addition to established categories of sensitive information (such as precise information relating to past, present or future health conditions or treatment) this provision now incorporates new forms of potentially sensitive information, such as information describing precise real-time geographic location.
- The Children's Online Privacy Protection Act is extended to the realm of non-personally identifiable information, whereby verifiable parental consent is now required for any use of non-PII or PII to create an interest segment for behavioral advertising that is specifically targeted to children under 13.
- The 2008 Self-Regulatory Code expands the commitment of NAI members to provide reasonable security for all types of data used for behavioral advertising (including non-personally identifiable information), and establishes a baseline for retention of such data.
- Finally, the 2008 Code establishes a commitment to an in-house compliance review to be published annually, as well as to a consumer complaint process to regularly review questions about members' compliance.

---

[20] *See* the Network Advertising Initiative's 2008 Self-Regulatory Code of Conduct, *available at* http://www.networkadvertising.org/networks/principles_comments.asp.

[21] *Id.* at Section III (2) (b) (members shall require that Web sites "clearly and conspicuously post notice – or ensure that such notice be made available on the web site where data are collected . . . ."). Although Web site privacy policies today are the most widely-adopted and hence the most scalable and consistent means of achieving notice across thousands of Web sites of varying size and complexity, the Code is intended to anticipate possible innovation.

The current Self-Regulatory Code continues to leverage the principle of public attestation and potential regulatory accountability for deceptive practices – for a far larger group of NAI member companies. The NAI's reliance on such an attestation model mirrors that of other initiatives for the protection of user data, notably including the Department of Commerce's Safe Harbor Framework for the transfer of the personal data of European citizens.[22]

III. The **NAI's Continued Commitment to Effective and Flexible Self-Regulation**

The NAI and its members believe that self-regulatory approaches to online advertising should be as dynamic as the marketplace in which they operate. Input from consumers, policy makers, and industry is invaluable in identifying areas for the evolution of best practices for online behavioral advertising. Given their significant role as infrastructure providers for Web-based ad serving and data management across a broad cross-section of Web publishers and services, NAI members are well positioned to evaluate the technological challenges and opportunities to enhance consumer transparency and choice for HTTP cookie-based online advertising. Additionally, the NAI believes that its members' technological expertise can be invaluable to more rapid and consistent implementation of self-regulation of cookie-based advertising across the Internet ecosystem.

In February 2009, the FTC issued its Staff Report detailing "Self-Regulatory Principles for Online Behavioral Advertising." The NAI and its members have focused their recent efforts around several of its key recommendations:

A. Enhancing consumer notice mechanisms

The NAI 2008 Self-Regulatory Code requires its members to secure notice and choice for consumers on the Web sites on which their behaviorally-related advertisements appear. While as a practical matter such notice and choice is usually provided within a Web site's privacy policy (or a layered summary of the policy), the Code allows NAI members the flexibility to pursue any disclosure approach so long as companies ensure that clear and conspicuous notices are available to consumers on the websites where online behavioral advertising occurs.

Regulators and other thought leaders in the online advertising industry have suggested that consumer notice for online behavioral advertising might be enhanced through the provision of additional mechanisms that provide notice through the advertisement itself (i.e. by providing disclosures directly within, or immediately adjacent to, the ad).

Several NAI members have now either tested or actually deployed a variety of possible implementations of consumer notice in direct proximity to banner ads, which can inform potentially wider adoption by industry:

[22] *See, e.g.,* the U.S. Safe Harbor Framework's Annual Reaffirmation Requirement, *available at* http://www.export.gov/safeharbor/eg_main_018243.asp.

- AlmondNet offered a direct "Powered by Almondnet" hyperlink within behaviorally targeted banner advertisements for one of its product lines from 2004-2006, enabling consumers to access AlmondNet's opt-out choice more directly;
- Over the past 18 months Yahoo! has extensively tested a variety of implementations of notice "in or around" display advertisements, including with significant Web publishers such as eBay;[23]
- In March 2009, Google deployed clickable links to a consumer choice page directly within the display advertisements it serves;[24] and
- FetchBack, a retargeting company, last week also deployed direct links to its Privacy Center (a single location incorporating consumer information and its opt-out link) within the ads it serves.[25]

Adoption of a common approach to implementing such alternatives for notice of behavioral advertising presents a considerable challenge, both in terms of the technological complexity of the infrastructure and the great diversity of publishers and advertisers involved. Large Web publishers may prefer to develop customized site links for disclosure adjacent to banner advertisements, while smaller Web publishers may prefer ad serving companies to provide for disclosure within the ad banner itself. In seeking to implement notice options that supplement well-established mechanisms like privacy policies, the NAI also recognizes that considerable testing, research, and consumer feedback will be needed.

Notwithstanding these challenges, the NAI and its member companies believe that technologies should be developed and built to allow for enhanced notice by any entity engaged in online behavioral advertising. The NAI and its member companies are now actively engaged in technical discussion of the infrastructure approach that would best facilitate such enhanced notice. A working group of NAI member technologists has been established to promote compatible approaches to the delivery of such enhanced notice; to identify and refine possible infrastructure standards to support flexible consumer disclosure formats; and to consult with other interested providers and associations on the best way to ensure technological compatibility.

Additionally, the NAI has been actively engaged in a cross-industry associations process involving advertisers, publishers, and marketers to develop industry-wide self-regulatory

---

[23] An example of eBay's implementation is *available at* http://cgi6.ebay.com/ws/eBayISAPI.dll?DisplayAdChoice&w=1&y=3FwEhZwEEKTEEUCxpAAAsPQEEKVgCVC1RU1YtDlcCeA0AV3k%3D (accessed June 15, 2009).

[24] *See* Nicole Wong, Google Public Policy Blog, *Giving Consumers Control over Ads* (March 11, 2009), *available at* http://googlepublicpolicy.blogspot.com/2009/03/giving-consumers-control-over-ads.html.

[25] *See* Press Release, *FetchBack to Provide Enhanced Notice in Behavioral Ads* (June 15, 2009), *available at* http://www.fetchback.com/press_061509.html.

principles for online behavioral advertising.[26] The participation in this process of representatives of thousands of companies within the Internet ecosystem represents a potentially significant widening of the self-regulatory approach to behavioral advertising issues long supported by the NAI. The NAI and its members are committed to supporting this initiative, as well as to promoting the deployment of enhanced notice mechanisms.

B. Improving the durability of cookie-based opt outs

The NAI's opt-out tool presently allows consumers the choice whether to receive behaviorally-related advertising from some or all NAI members, and have that choice apply across the many Web sites served by each of NAI member companies.

The opt-out mechanisms implemented by the NAI and its members generally use industry standard Web browser cookies to record these preferences. The cookie helps ad networks "remember" the opt-out preference by storing it on the browser of the user's computer. The use of cookies either for advertising or for opt-out purposes share a common potential technological limitation: if a user deletes such cookies from the Web browser cache on the user's computer, or deploys computer software that automatically deletes such cookies, user preference data previously connected to the particular browser though the cookie is lost. Recent work by NAI member companies and other technologists have demonstrated the potential of enhancing the durability of consumer opt-out preferences through the deployment of browser plug-ins. Such browser plug-ins attempt to solve the problem of opt-out cookie deletion by automatically reinstating such cookies each time the browser cookie cache is emptied, or the opt-out cookie is otherwise deleted (*e.g.*, by antispyware programs that do not distinguish between the various purposes for third party cookies).

The NAI believes that technology should be deployed in connection with NAI members' existing commitments to offer opt-out choice to consumers, so as to enhance users' ability to preserve the opt-out preferences stored in their browsers. This summer the NAI intends to make available through its opt-out Web page additional technology that would protect opt-out cookies from deletion, and that would leverage a recognized list of opt-out cookies from NAI members. This approach would afford users a more convenient means for having their Web browsers remember their opt-out preferences.

C. Continued education to improve consumer awareness

User education about advertising technologies and their choices remains a vital foundation for the continued viability of online behavioral advertising. NAI members have a demonstrated commitment to consumer education about online advertising. Several NAI member companies have already experimented with education initiatives in video, banner, and text form to help bolster public understanding of the benefits of online

[26] *See* Press Release, *Key Advertising Groups to Develop Privacy Guidelines for Online Behavioral Advertising Data Use and Collection* (January 13, 2009), *available at* http://www.iab.net/about_the_iab/recent_press_releases/press_release_archive/press_release/pr-011309.

behavioral advertising and the choices that consumers have in connection with such advertising.[27]

NAI member companies, especially ad networks, are well positioned to deliver consumer education across a great diversity of web sites. The reach of NAI member advertising networks creates a footprint for the broadest possible online audience. Moreover, given the NAI's focus on issues of consumer transparency and choice for online behavioral advertising, the NAI member companies are particularly well suited to promote consumer education specifically focused on the transparency and choice issues associated with browser-based behavioral advertising.

The NAI recently launched a new consumer education web page (http://networkadvertising.org/managing/learn_more.asp), which aggregates video, blog and explanatory content, together with information relating to general research and public policy discussion. Starting this month, the NAI is deploying educational banner links across participating NAI member companies' ad networks. Promotions may be of members' own education campaign materials, the NAI's, or any other entities' consumer-facing materials addressing online behavioral advertising and available consumer choices.

The NAI expects to take an interactive approach with consumers, factoring consumer input into its educational efforts on an ongoing basis. Moreover, the NAI also plans to coordinate its educational efforts with other initiatives by industry to promote common objectives of consumer awareness, particularly as those efforts may evolve to include initiatives such as enhanced advertising notice.

IV. Conclusion

The NAI thanks the Members of the Subcommittees for the opportunity to discuss the workings of its members' online behavioral advertising technologies, and the economic benefits they provide to ad-supported Wed publishers and the consumers of these services. Public discussion of the privacy issues associated with online behavioral advertising remains a vital means for determining the appropriate focus of industry efforts to promote appropriate transparency and choice. The NAI and its members look forward to working constructively with the Subcommittees as they consider these important issues.

[27] *See, e.g.*, AOL's privacy education site, *at* http://www.privacygourmet.com. Google also maintains a privacy channel at YouTube, *at* http://www.youtube.com/user/googleprivacy?blend=2&ob=1.

Mr. RUSH. The chair thanks the gentleman. Now the chair recognizes Mr. Cleland for 5 minutes.

TESTIMONY OF SCOTT CLELAND

Mr. CLELAND. Thank you, Mr. Chairman, both you and the ranking member. As a leading Internet expert and consultant, I obviously have Internet companies as clients, which include wireless cable and telecom broadband companies in the communications sector, and Microsoft in the tech sector. However, I want to emphasize my views today are my personal views and not those of any of my clients. What I want to do is talk about the Internet problem and Internet solution. So what is the Internet privacy problem? Well, technology has turned privacy upside down. Before the Internet, it was inefficient, it was costly, and it was difficult to collect private information. Now it is hyper-efficient, cheap and easy to invade privacy. So through inertia what we have is a default, finders keepers, losers weepers, privacy policy.

Now, second, most Americans incorrectly assume that the privacy they enjoyed offline in the past is the privacy they have online, and that is not true. Third, all the technology megatrends out there, social networking, cloud computing, Internet mobility, Internet of Things, all of them will dramatically increase privacy risks online. Fourth, there is a significant faction in the technology community that really views privacy negatively and in some parts antithetical to the behavioral advertising and the Web 2.0 model. Now, fifth, a problem is that increasingly the underground currency of the Internet is private data. Now private information is very valuable, but in the absence of a system where consumers can assert ownership and control over their private information, privacy can be taken away from them for free and profited from with no obligation to or compensation due to the affected consumer.

The sixth part of the problem, and that is we now have a technology-driven Swiss cheese privacy framework, which may be the worse of all possible worlds. Simply, the haphazard framework we have gives a user no meaningful informed choice to either protect themselves or benefit themselves in the market place arena of their private information. So what is the solution? I think it is very simple. You have a consumer-oriented, consumer centric approach that is technology and competition neutral. Think about it. It is consumers' private information that is being taken and exploited without their consent. Since it is consumers that are most at risk of having their information misused or stolen, wouldn't it be logical for our privacy framework to be organized around the consumer?

Now, clearly, businesses should be free to fairly represent and engage consumers in a fair market transaction for their private information. Now its fair market transaction where consumers are able to effectively understand and negotiate the risk and reward involved with sharing the private information. Moreover, since the consumer is the only one that knows which information about their personal situation or their views or their intentions or their interests, which ones they are comfortable with sharing, shouldn't it be the consumer that is empowered to make those decisions? So if Congress decides that it is going to legislate in this area, I think one thing is obvious, and that thing is that you should have con-

sumer framework that would be superior to the current technology-driven framework. That is because it would emphasize protecting people, not technologies. It would empower consumers with both the control and the freedom to choose to either protect or to exploit their privacy.

It would prevent competitive arbitrage by creating a level playing field. And it would allow you to stay current with the constant changing innovation because you are not technology oriented, you are consumer oriented. And, lastly, you are going to be able to accommodate both sides, the people who care very much to protect their privacy but also those who care less and would like to exploit their private information. So in closing I think we can do better than the current finders keepers, losers weepers privacy policy that is the de facto policy of the United States. Thank you, Mr. Chairman, and ranking member for the opportunity to testify.

[The prepared statement of Mr. Cleland follows:]

Summary Testimony of Scott Cleland, President, Precursor LLC
"Why A Consumer-Driven, Technology/Competition-Neutral, Privacy Framework Is Superior to a Default 'Finders Keepers Losers Weepers' Privacy Framework"
Before the Joint House Energy & Commerce Hearing on Behavioral Advertising, June 18, 2009

Precursor LLC is an industry research and consulting firm specializing in the future of the converging techcom industry. For the last three years, I have also been Chairman of NetCompetition.org, a pro-competition e-forum funded by broadband companies. In addition, beginning in 2009, I have done consulting for Microsoft. **My testimony today reflects my own personal views and not the views of any of my clients.**

The Privacy Problem:

- *First,* **technology has turned privacy reality upside down.** Before the Internet most people enjoyed substantial privacy because it was inefficient, difficult and expensive to collect and disseminate private information. However, Internet technology has flipped that reality on its head by making it hyper-efficient, easy and near free incrementally to collect and disseminate private information. As a result, **we now have a technologically/competitively-skewed, *"finders keepers losers weepers"* privacy framework by default.**
- *Second,* the essence of the behavioral advertising or Internet privacy problem is captured well by the Consumer Reports 9-25-08 poll which spotlighted that **the average American consumer believes they are in much more control of their private information online than in fact they are.**
- *Third,* all of the technology megatrends (social media, cloud computing, Internet mobility, and the Internet of Things) are all converging to increase the risks to consumers who wish to safeguard their privacy online.
- *Fourth,* there is a growing collection of "publicacy" interests among the technology elite that view privacy online very differently than most Americans view privacy offline. Increasingly, Congress will be forced to weigh these increasingly competing and conflicting online/offline privacy interests and trade-offs.
- *Fifth,* **increasingly the "underground currency" of the Internet is private data.** Private information is valuable, because in the absence of a system where consumers can assert ownership of and control over their privacy, privacy can be taken from them for free and profited from with little to no obligation to, or compensation due, to the affected consumer. The increasing commercialization of privacy by publicacy businesses increasingly creates new risks for consumers in return for little to no protection or reward.
- *Finally,* **the current technology-driven, "Swiss cheese" privacy framework may be the worst of all possible worlds.** In the absence of a consumer-driven, technology/competition neutral, privacy framework, consumers have neither a meaningful role in protecting their privacy nor the freedom to exploit some of the value of their private information -- if that is their choice. Simply, the current haphazard privacy framework affords an individual no meaningful-informed choice to either protect or benefit themselves in the marketplace arena of their private information. The technology used should be irrelevant to privacy policy.

A Privacy Solution: A Consumer-Driven, Technology/Competition-Neutral Privacy Framework:
Since it is consumers' private information that is being taken and exploited without much meaningful consent by the consumer, and since it is consumers which are most at risk from having their most private information stolen or used inappropriately, wouldn't it be more logical for a privacy framework to be more oriented around a consumer' perspective rather than a technology perspective? Clearly businesses should be free to fairly represent and engage consumers in a fair market transaction over the disposition of their private information -- a fair market transaction where consumers are able to effectively understand and negotiate the risk/reward value of sharing their private information. Since a consumer is the only one who knows what information about their personal situation, interests, views and intentions, they are comfortable in sharing for what purposes, wouldn't it be logical to have a privacy framework that empowered consumers with real input and influence over either protecting or exploiting their own interests, whatever they may be?

Conclusion: *If* Congress decides to legislate on Internet privacy, a consumer-driven, technology/competition-neutral privacy framework would be superior to a technology-driven privacy framework, because it would:

- Emphasize protecting people not technologies;
- Empower consumers with the control/freedom to choose to either protect or exploit their own privacy;
- Prevent competitive arbitrage of asymmetric technology-driven privacy policies with a level playing field;
- Stay current with ever-evolving technological innovation; and
- Accommodate both privacy and publicacy interests by empowering real consumer privacy choice.

Written Testimony of
Scott Cleland
President, Precursor LLC

"A *Consumer-Driven, Technology/Competition-Neutral Privacy Framework Is Superior to a Default 'Finders Keepers Losers Weepers' Privacy Framework*"

Before the
House Energy & Commerce Subcommittees On:
Communications, Technology, and the Internet
&
Commerce, Trade, and Consumer Protection

Joint Hearing on:
"*The Potential Privacy Implications of Behavioral Advertising*"

June 18, 2009

I. Introduction

Mr. Chairmen and Members of the Subcommittees thank you for the honor of testifying on the important subject of: "*The Potential Privacy Implications of Behavioral Advertising.*" I am Scott Cleland, President of Precursor LLC, an industry research and consulting firm, specializing in the future of the converging techcom industry. For the last three years, I have also been Chairman of NetCompetition.org, a pro-competition e-forum funded by telecom, cable and wireless broadband companies. In addition, beginning in 2009, I have done consulting for Microsoft. **My testimony today reflects my own personal views and not the views of my clients.**

My purpose today is to help the Subcommittees see the business of behavioral advertising through the lens of consumer/user privacy. At core, behavioral advertising is the commercialization of privacy or "publicacy." "Publicacy" is simply the antonym or opposite of privacy. Increasingly, private information is becoming a de facto underground currency of the Internet.

A wide range of Internet and behavioral advertising trends are coalescing to force Congress to grapple with some fundamental public policy questions with regard to privacy:

1. Is respect for privacy still important and relevant in America in the Internet Age?
2. Is an individual's privacy or freedom from intrusion, more or less important than others' freedom to uncover private information and make it public without permission?
3. Do American's have the right to own and control their own private information, in order to either protect or benefit their selves?
4. To what extent should accountability exist for violating expressed right to privacy?
5. What overall privacy framework is the most appropriate, effective and adaptable in the Internet Age?

The outline of my testimony is as follows:

I. Introduction
II. Trend Convergence
III. The Privacy Problem
IV. A Privacy Solution
V. Conclusion

II. Trend Convergence

Privacy norms and expectations developed over decades in the physical world are rapidly being over taken by events in the virtual or Internet world. Increasingly a convergence of many Internet and behavioral advertising trends is undermining consumer expectations of respect for privacy.

Consumer Expectations Trends: The first and maybe most relevant trend to the Subcommittees is that most consumers are largely unaware that they are not in control of their private information online. For example, a Consumer Reports 9-25-08 consumer poll found:

- *"61% are confident that what they do online is private and not shared without their permission;*
- *57% incorrectly believe that companies must identify themselves and indicate why they are collecting data and whether they intend to share it with other organizations;*
- *48% incorrectly believe their consent is required for companies to use the personal information they collect from online activities..."*
    - http://www.consumersunion.org/pub/core_telecom_and_utilities/006189.html

Technology Trends: Second, is the well-known trend of Internet convergence which has an outsized impact on privacy because Internet convergence enables for the first time the widespread and micro-detailed collection, storage, aggregation, access, analysis, sharing, distribution, and commercialization of any digitizable form of private information (e.g. data, text,

image, video, voice, click-streams, etc.). Simply, the Internet has enabled the potential for unprecedented invasion of privacy.

- Moreover, all the biggest Internet technology megatrends will only exacerbate privacy concerns over time because:
  - *The Web 2.0 Social Media megatrend* often views respect for privacy as "friction" and an impediment to "open" sharing and community-building on the Internet;
  - *The Cloud Computing megatrend* of outsourcing data processing and storage elsewhere to the "cloud" and not on an individual's desktop or laptop, often views respect for privacy as a cost and an inefficiency;
  - *The Internet Mobility megatrend* of accessing the Internet anywhere wirelessly and not just through a tethered stationary connection, increasingly impacts respect for privacy because it can enable others to know users' exact locations and to track where they go or have gone; and
  - *The Internet of Things megatrend* of assigning web addresses to sensor-chips on objects or physical things impacts privacy in that it could make public private property as never before.

Publicacy Attitude Trends: Third may be the trend that Congress is probably least aware of, the emergence of "publicacy" attitudes in the technology community. Before the Internet, there was no need for an antonym for privacy or a new word that captured being opposed to or in conflict with privacy. That's because in the past there simply weren't significant forces working against respect for privacy as there are today. I coined the term "publicacy" in my previous Internet privacy testimony before this Subcommittee to spotlight and help Congress understand that the only way to fully understand the evolving issue of Internet privacy is to understand the new emerging Internet trends and attitudes that are increasingly in tension with well-established privacy norms and expectations in the physical world.

- The origin of "publicacy" attitudes that digital private information should not be viewed as personal property that requires permission to use may be rooted in part in the Free Software Foundation's definition of Free Software: "*Free software is a matter of the users' freedom to run, copy, distribute, study, change and improve the software. ... Being free to do these things means... that you do not have to ask or pay for permission.*"

- Some in the Information Commons movement appear to have expanded the Free Software notion that "*you do not have to ask or pay for permission*" from software code to include most content created online. To the extent that interactions occur in the so called "public" domain of the Internet, the Information Commons movement tends to see that information as public even if others may consider it private information.
- Some in the Web 2.0 Social Media movement, appear to have further expanded on the notion that "*you do not have to ask or pay for permission*" from most content created online to community building and sharing online. Asserting one's privacy in this context is looked upon by some in the social media movement to be the opposite of sharing, and not being open and transparent.
- On top of these emerging attitudes, many in the behavioral advertising business community have viewed respect for privacy as a friction, an inefficiency or an impediment to business models based on perfecting the efficient targeting or relevance of online advertising.

Commercialization of Privacy Trends: Finally, is another trend that Congress may not be as aware of as they may want to be – that is -- why is there such a driving force to commercialize privacy online? What makes private information so valuable?

- Private means economically rare or having scarcity value. Value increases with the amount of scarcity.
- Private can mean a secret weakness/vulnerability that someone does not want to be revealed and would pay to keep private.
- Private information now can be efficiently and effectively collected, skimmed, mined, analyzed and disseminated via automation at exceptionally low incremental cost or transactional friction on the Internet.
- Private information can be arbitraged for competitive advantage.
- What can make intrinsically valuable private information even more valuable?
    - No one else has it or can get it.
    - No one knows one has it so they can use it secretly to not arouse suspicion, alarm, or distrust.

- Not having to share any of the value creation from the private information with the owner of the private information.

The commercialization of privacy is becoming increasingly sophisticated. In essence, the long-held sales and marketing axiom of know thy customer/target is morphing online from an art to a science to ultimately math.

Overall, the convergence of these trends: consumer expectations, technology, publicacy attitudes and commercialization of privacy – all suggest increasing pressure on Congress and the legislative process to sort out these increasingly conflicting interests.

III. The Privacy Problem

First, technology has turned privacy reality upside down. Before the Internet most people enjoyed substantial privacy because it was inefficient, difficult and expensive to collect and disseminate private information. However, Internet technology has flipped that old reality on its head making it hyper-efficient, easy and near free incrementally to collect and disseminate private information. **As a result we have moved from a stable respect for privacy framework to an unstable, technologically/competitively-skewed, *"finders keepers losers weepers"* privacy framework.**

Second, the essence of the behavioral advertising or Internet privacy problem is captured well by the Consumer Reports 9-25-08 poll which spotlighted that the average American consumer believes they are in much more control of their private information online than in fact they are. The obvious implication for Congress is that American consumers' guard is way down and that they either need to be better informed about their increasing lack of privacy online or afforded more choice to better protect or benefit from their private information online.

Third, all of the technology megatrends (social media, cloud computing, Internet mobility, and the Internet of Things) are converging to vastly increase the risks to consumers who wish to safeguard and protect their privacy online.

Fourth, there is a growing collection of publicacy interests among the technology elite that view privacy online very differently than most Americans view privacy offline. Increasingly, Congress will be forced to weigh these increasingly competing and conflicting online/offline privacy interests and trade-offs.

Fifth, increasingly the "underground currency" of the Internet is private data. Private information is valuable to many Internet businesses, because in the absence of a system where consumers can assert ownership of and control over their privacy, privacy can be taken from them for free and profited from with little to no obligation to, or compensation due, to the affected user/consumer. In effect, the increasing practice of commercializing privacy by publicacy businesses increasingly creates new risks for consumers in return for little to no protection or reward.

Finally, the current technology-driven, "Swiss cheese" privacy framework may be the worst of all possible worlds. In the absence of a consumer-driven, technology/competition neutral, privacy framework, consumers have neither a meaningful role in protecting their privacy nor the freedom to exploit some of the value of their private information -- if that is their choice. Simply, the current haphazard privacy framework affords an individual no meaningful-informed choice to either protect or benefit themselves in the marketplace arena of their private information.

The current technology-driven privacy framework ironically puts privacy and consumers last; the technology used should be irrelevant to privacy protection. Even more ironic, it also can be decades out-of-date with technology advances. Technology-driven privacy is all about what's best for the technology model -- consumers are an afterthought. The ultimate irony here may be that the Internet publicacy interests that say they believe in empowering end users with choice often are opposed to empowering end-users/consumers when it comes to privacy choice.

IV. Solution: Consumer-Driven, Technology/Competition-Neutral Privacy Framework

Since it is consumers' private information that is being taken and exploited without much meaningful consent by the consumer, and since it is consumers which are most at risk from having their most private information stolen or used inappropriately, wouldn't it be logical for a consumer privacy framework to be more oriented around a consumer's ongoing perspective rather than the technology snapshot perspective of a particular point in time?

- Clearly businesses should be free to fairly represent and engage consumers in a fair market transaction over the disposition of their private information -- a fair market transaction where consumers are able to effectively understand and negotiate the risk/reward value of sharing their private information.
- Since a consumer is the only one who knows what information about their personal situation, interests, views and intentions, they are comfortable in sharing for what purposes, wouldn't it be logical to have a privacy framework that empowered consumers with real input and influence over either protecting or exploiting their own interests, whatever they may be?

Isn't it logical for consumer privacy to be a matter of a consumer's meaningful individual choice?

V. Conclusion:

The essence of the Internet privacy problem is that technology has turned privacy reality upside down. Before the Internet most people enjoyed substantial privacy because it was inefficient, difficult and expensive to collect and disseminate private information. However, Internet technology has flipped that old reality on its head by making it hyper-efficient, easy and near free incrementally to collect and disseminate private information. As a result we have moved from a stable respect for privacy framework to an unstable, technology-driven, "*finders keepers losers weepers*" privacy framework – by default.

Consequently, Congress faces some big and important decisions.

- Should technology or people decide if there is respect for privacy?
- Is respect for privacy still important in the Internet Age?
- If so, should Americans be able to largely own and control their private information?
- Is an individual's right to privacy online of greater or of less importance than Internet openness and transparency?
- Is a consumer-driven or technology-driven privacy framework better for Americans?

If Congress decides to legislate on Internet privacy, a consumer-driven, technology/competition-neutral privacy framework would be superior to a technology-driven privacy framework, because it would:

- Emphasize protecting people not technologies;
- Empower consumers with the control and the freedom to choose to either protect or exploit their own privacy;
- Prevent competitive arbitrage of asymmetric technology-driven privacy policies which harms consumers with a competitively neutral, level playing field;
- Stay current with ever-evolving technological innovation; and
- Accommodate both privacy and publicacy interests by empowering consumers to individually decide how they want to protect or exploit their private information (from strong broad privacy protections, to tailored protections, to free use of their private information.)

Thank you again Mr. Chairmen for the opportunity to share my personal views and analysis on "*The Potential Privacy Implications of Behavioral Advertising.*"

Mr. RUSH. The chair thanks the gentleman. Now the committee will engage the witnesses in a series of questions, and the chair recognizes himself for 5 minutes for the purpose of questioning the witnesses. Ms. Toth, in your testimony you discuss meaningful choice for consumers, and this is a principle that everyone agrees is a good one. However, it appears that the only choice for consumers using Yahoo! is to opt out of receiving "interest-based advertising." It seems that they can't opt out of Yahoo!'s collection of information and tracking. Can you clarify exactly what the consumers' choice is with Yahoo!'s opt out? If consumers ask to opt out of behavioral advertising, does your company continue to collect data on their browsing habits?

And I have another question. Does the opt out only stop the displaying of targeted advertising or does it stop the collection of data? Does your firm offer consumers any way to opt out of tracking and data collection? Would you answer those three questions for me, please?

Ms. TOTH. Our opt out, you are correct, it is not an opt out of collection of data. It is an opt out of use of data. So there are a number of reasons why we collect data and primarily that relates to the display of advertising, so advertisers pay us to show advertisements, and so we have to know if those ads were delivered and shown so we collect information in order to report that information back to the advertisers who are paying for those ads. But another reason why has a lot to do with the way we operate our web site, so if we were to stop collecting data when a user opts out then there are a number of users we suspect would opt out and engage in behaviors on the site that may not be legitimate behaviors that may be abusive or fraudulent behaviors. So we are continuing to collect information, but when the user opts out we are no longer showing them behavioral advertisements. We are opting them out of that use of their data.

So we are a web site that offers a number of different services. Ad serving is one of our many businesses, so we have other uses for the data as I described. I am not sure if I understood the other question specifically as being different from that one. I maybe misheard. So the extent that data is no longer used for advertising, that is what the opt out applies to. But the opt out that we offer is actually a very—it is very clearly provided to users, and it is actually very easy to find, so we think that that actually matters a great deal. The other thing actually that I will mention is that what we offer on the back end is anonymization of that data within 90 days so if users have a concern that there is a great deal of data being collected, we hope to be addressing that on the back end by anonymizing the vast majority of our data within 90 days.

What is really notable about that is that our policy doesn't just apply to search log records or to a specific type of log file that all of our log systems including the log systems that inform our advertising capabilities.

Mr. RUSH. So a consumer cannot opt out of data collection at all?

Ms. TOTH. The consumer can't opt out through——

Mr. RUSH. Cannot. They cannot opt out of data collection.

Ms. TOTH. No. There are other tools at the browser level that would address that. Our systems don't work that way.

Mr. RUSH. Ms. Wong, can you answer the same questions for me?

Ms. WONG. Sure. Let me start by sort of describing our approach to privacy and data collection on our sites generally because I don't know if you are a regular Google user. Google actually has a design philosophy of always trying to minimize the amount of data we collect about a user in the first instance, so almost all of our services actually don't require a user to provide any personal information at all. When you go to Google Search, you don't have to register. You simply type in your search. If you type in a search and you are not signed in or registered with us what that means is the only thing we get back is what all of us here, what all web sites get, which is sort of a standard what we call log line that records—a computer is asking you a question and that question comes with two things that can be identifying a user. One is an IP address, which your ISP assigns to you, and the other is a cookie, which is what Anne referenced.

Neither of those things for Google are tied to an individual. You can't know it is Nicole or Chris or Anne based solely on the IP address and the cookie. Just to be clear about the type of data we collect, we do provide an opt out, as I was demonstrating in our presentation, for the use of that cookie and IP address data to target ads. In other words, when you click on the opt out what it does is instead of getting a unique cookie, which is a series of numbers and letters, what you get is what we call the opt out cookie, and that opt out cookie literally says in it opt out so that the data that we collect goes into a huge pool of all users who have the same opt out cookie. It is completely abrogated which means we can't see an individual user in that pool of data that has been identified as opt out.

Mr. RUSH. The chair's time is up. The chair now recognizes the ranking member, Mr. Radanovich, for 5 minutes, and at the conclusion of his questions and answers, the chair will relinquish the chair to the chairman of the Communications Subcommittee at that point.

Mr. RADANOVICH. Thank you, Mr. Chairman, and welcome members of the panel. Your testimony is very interesting. My first question goes to Mr. Curran, is it? For your testimony, I understand that you are involved in a broad industry-wide effort to create self-regulating principles, and that these principles, you are going to be releasing these principles pretty soon, I understand within about 30 days. Can you expand a little bit on what we can expect you to address on those, and I am particularly interested about the enforcement areas of these principles.

Mr. CURRAN. Actually I think there are two different answers to your question because there are two different things going on, and in my long form testimony I detailed some of the work going on with the NAI in terms of our member companies, which are primarily advertising networks and other online marketing companies, to essentially further the development of technology that will allow, as Ms. Wong showed you with her presentation, notice inside the banner ad really to get together to advance an infrastructure that would allow any entity serving a behaviorally targeted ad or any party responsible for a behaviorally targeted ad to deliver that kind of notice in connection with an ad.

Mr. RADANOVICH. So that is work that the NAI has been pursuing from a technological perspective?

Mr. CURRAN. Separately, I think your question relates to a far broader industry dialogue that has been not led by the NAI but instead by the IAD, the DMA, the AAAA's, the ANA, and also the BBB. That is a lot of acronyms.

Mr. RADANOVICH. That is much clearer now.

Mr. CURRAN. I think the key takeaway here is that certainly the FTC has indicated that broader self-regulatory approaches were needed for industry, and that is very much an effort in that direction of actually establishing principles similar in spirit to those of the NAI to apply on an ecosystem wide basis. My understanding is that the roll out of those principles is in weeks. And we are very much supportive of those efforts, and I think they are very much a part of a trend of really a momentum towards exactly what the FTC called for in terms of really a very vigorous engagement.

Mr. RADANOVICH. Thank you very much. Ms. Wong, I would love to ask you a question regarding your comments or support of establishing a uniform online and offline framework for privacy. Now I would love to have you clarify what uniform means and does it mean that it should apply to all entities and engage in collecting or using and sharing online information whether they are ISPs or application providers? Should it be straight across the board or are there different applications?

Ms. WONG. Yes. And I think there are two answers to that. As an initial matter, Google and a number of the folks at the table here have been really working hard to think about federal comprehensive privacy legislation, and if I were to encourage the committee to do anything I think it is backing something like that because our history on privacy legislation has really been about sectorally trying to regulate privacy with children, with health, with financial, so that for a user on the Internet their Internet experience is seamless. They go from their bank to their doctor to their web service seamlessly and don't realize that different privacy laws apply. The important for ensuring that users continue to trust the use of their data on the Internet is to have baseline privacy law across industries. To get to your second question about——

Mr. RADANOVICH. Let me ask this and clarify it a little bit. When you say uniform, does that apply to content providers that provide content over Google? Would they be subject to the same—is that what you call uniform online privacy?

Ms. WONG. Right. So, yes, there would be baseline standards for all companies in terms of notice to users, access and control for users, and security for that data.

Mr. RADANOVICH. OK. Thank you. Ms. Toth, in Yahoo! recently you announced that you will completely erase IP addresses at the end of its data retention period rather than just deleting a few numbers as is the practice of a number of your competitors. If you don't need the IP addresses for fraud prevention or anything else, what is the utility in keeping the IP address at all, and why the fractional numbers of why don't you just dump it right away?

Ms. TOTH. I think we actually have slides in there of our data retention policy and the process steps that we take so for the vast majority of our data at 90 days we de-identify the data. We apply

a four-step process to remove identifiers. The IP address is one of those identifiers that is stored in the logs, and for us we completely delete that identifier at 90 days with the exception of the fraud and abuse systems which hold it for up to 6 months and then it is deleted. So we store that data only for as long as we need it for the purposes of providing our services and then we de-identify the records and that gets to the IP address. The IP address is typically in the context of use have more to do with customizing a user's experience along the lines of geography, those sorts of things. But it is de-identified and it is removed at 90 days. Does that answer your question?

Mr. RADANOVICH. Good enough. Thank you very much.

Mr. BOUCHER [presiding]. Well, I again want to express apologies to our witnesses for the lengthy delay. We were on the House floor a bit longer than we had anticipated, and you were very patient. We want to express the committee's appreciation to you for your willingness to stay with us and provide what has been some truly excellent testimony. I am going to propound a series of questions and then recognize other members who are here. Some have made the point in written testimony, and I have heard it made otherwise, apart from this hearing, that there can be a meaningless opt in and a meaningful opt out. And I would assume that the difference with regard to meaningfulness depends to some extent on the degree of disclosure that is made to the user. So what I would like is to get your statement of what you think the elements of a meaningful opt out would be. Who would like to answer? Mr. Chester.

Mr. CHESTER. I would like to say, thanks, that I think we need an opt in. And my rule of thumb is, and this has to be done in a doable way to make——

Mr. BOUCHER. Mr. Chester, before you alter the question and answer the question you wish I had asked, let me see if we can get you or someone to answer the question I actually did ask. Ms. Wong.

Ms. WONG. I will give it a try. And I agree with the concept of there are good opt outs and there are bad opt ins. I think a bad opt in is, you know, an opt in slipped in in a long provision at the beginning of a contract relationship with your user that they forget over time, and so there could be continued data collection in the life of your relationship with that user that the user completely forgotten about. A good opt out is an opt out that is presented again and again to the user as a meaningful choice to them. So in our interest-based advertising, for example, one of the things that we are trying to do is to put ourselves in front of the user so that we encourage them to engage with their own data. That is the purpose of that Ads by Google link in the ad because we want them to know when you are looking at this page it is not just the New York Times you are looking at. The ad is from Google, and you should engage with that data. The purpose of our ads preference manager is again to give the users a sense of control so that they change their behavior and start to engage and take control of their own data. And I think that——

Mr. BOUCHER. So you would make full disclosure to the user of what information is collected about the user. You would describe

how that information is used once you have collected it and then you would provide the opt out opportunity?

Ms. WONG. That is right.

Mr. BOUCHER. And would those be the meaningful elements of opt out as far as you are concerned?

Ms. WONG. I think that is right. The continued engagement with the user.

Mr. BOUCHER. All right. Now let me ask Mr. Chester, who I know is very interested in taking part in this discussion, what his response to that would be.

Mr. CHESTER. Well, my rule of thumb is this, it has to be done workably. The companies should be telling the consumer what they tell perspective clients. When you see what—and I included some of that in my testimony, when you see what they are telling their clients and their perspective clients or when they are reporting on the results of the data collection system they have created with the advertising, they are talking about massive collection of data that is far beyond the ken of what might be presented in a simple opt out. So they need to be honest and tell people exactly what is about to happen. It can be a scale here, but if you read what they are doing including, frankly, the companies here, if you read what they are saying and also how the applications, the interactive applications, when you read the literature, the interactive applications have been designed, the online video, to get people to give up more data, so they have to be honest.

Mr. BOUCHER. All right. Thank you very much. If we were to draw a regulatory line of some sort that is focused on the collection and use of personally identifiable information, should we include within the definition of what is personally identifiable information, the IP address? Mr. Chester is saying yes. Let me see if any have any different views. Everyone agrees that—well, OK, Ms. Wong.

Ms. WONG. I will give it a try again. I think our position is that the IP address can be personally identifying depending on your relationship with the user so, for example, if you are the ISP that assigned that IP address what it means is that you are actually billing that user every month and having credit card or billing information from them, which means you can in fact associate the IP address, the ISP assigned, with a real person. If you are in a position like Google with an unauthenticated user where you don't know who is attached to an IP address it is not personally identifiable.

Mr. BOUCHER. So you are saying it would be personally identifiable if it is associated with other kinds of information about the user?

Ms. WONG. That is right.

Mr. BOUCHER. Some of which might be quite sensitive and personal.

Ms. WONG. That is right.

Mr. BOUCHER. You would probably say it is not personally identifiable if you have that in isolation perhaps with an opt out cookie?

Ms. WONG. Right.

Mr. BOUCHER. All right. I think I understand your position. In the time I have remaining, let me ask about the possible role that self-regulatory organizations might play in a statutory scheme that

would extend privacy rights to Internet users. Several questions about that. I know we have well-regarded SROs in existence today. Many of the major Internet companies are affiliated with one or more SROs, and I am concerned if we add a statutory scheme on top of that in order to assure that every Internet user has the understanding that his online experience is secure because all web sites will have to comply with a certain set of fundamental privacy assurances. How we do that in association with continued viability and usability for the SROs so just a couple of key questions. How would a user who feels aggrieved because the SRO, for example, may not have complied with the principles it signed up to comply with get recourse? Should there at some point be access to a federal agency to seek that resource? And how could we make sure that every web site actually complies with the minimum set of guarantees? So who would like to try answering that? Mr. Cleland.

Mr. CLELAND. Well, I think, you know, you are trying to get to something that actually works, and I think you are trying to get to an accountable system. One idea I would offer whether it is self-regulatory or governmental is that there needs to be some audit that is occurring on a regular basis. Those could be automated audits or they can be personalized. They need to be random because what you are talking about is meaningful. We are talking about accountable. And if you care about those two words and those two concepts and principles, there needs to be some verification.

Mr. BOUCHER. Other comments, Mr. Chester?

Mr. CHESTER. There is a role for self-regulation, but I just have to underscore that self-regulation has failed. The only reason the NAI is upgrading its principles is because of the controversy that occurred over the Google-DoubleClick merger when all these consumer privacy groups made so much trouble that then the FTC said, OK, we got to do something about privacy principles, and then the NAI after many years of being asleep, you know, decided, OK, we are going to revamp them. The only reason the companies have reduced their retention time is because the European Union has been pressing them. So it is the forces of regulation that have actually bolstered the failing self-regulatory system.

Mr. BOUCHER. So you would agree, would you not, Mr. Chester, that if the statute imposed certain fundamental guarantees and they meet your definition of what those fundamental guarantees of privacy should be, for example, that an SRO that enforces those fundamental guarantees or has those as its core principles that are a condition of membership, such an SRO could be effective, could it not?

Mr. CHESTER. I think the history of self-regulation certainly need telecommunications like the kids area has been that the self-regulatory structure is only as good as the law that has in fact——

Mr. BOUCHER. On that note, my time has expired. And I will recognize the gentleman from Florida, Mr. Stearns, for 5 minutes.

Mr. STEARNS. Thank you, Mr. Chairman, and let me also reiterate your comments. This is the first time I think in the history of Congress that we had this kind of procedure on the floor. We had almost 55 votes, and they were over almost 8 hours. And so you have hit sort of a perfect storm so your patience is appreciated and we appreciate you staying. Ms. Toth and Ms. Wong, on any

given day people come to your sites. Let us call that X. They all come to your sites. What percent of those people actually go to your privacy, Ms. Toth?

Ms. TOTH. We don't calculate it as a percentage. Overall, the number of page views of users who come to our privacy policy remains a fairly low number overall.

Mr. STEARNS. So let us say just take 1,000 people just to make it easy, 1,000 people. You couldn't even tell me if it is 10 percent or 1 percent or half a percent?

Ms. TOTH. It certainly is far lower than 1 percent.

Mr. STEARNS. So it is very, very small. And, Ms. Wong, how about you?

Ms. WONG. I don't know, and I can try and get back to you with the number, but off the top of my head I don't know the number of views.

Mr. STEARNS. No one on your staff can even just give a ballpark? I mean it is not 10 percent?

Ms. WONG. I am sure it is lower than the number of overall visits we get. Here is what I do know, which is that a year ago or so we started uploading videos to explain our privacy practices, and what we are seeing there is that users are engaging with us in those——

Mr. STEARNS. Because it is a video. OK.

Ms. WONG. Because it is a video and they are rating them and telling us what works for them and what doesn't, and I know that notice is a really important thing for this committee. We have to find better ways than a pure privacy policy to engage with our users to make them——

Mr. STEARNS. And videos might be a good way.

Ms. WONG. And videos——

Mr. STEARNS. Now each of you mentioned that you are willing to give to the consumer the information that you have collected and get it in sort of a category. And is this information that you are going to give—this is then sensitized or you have put together a summary and given it to the customer. Will you let the user actually see the raw data or at least actually see what you collect? Will you ever get to the point they can actually see what you collect?

Ms. TOTH. I would actually love it if we could—I would like you to see some of the data that we actually do collect because I think it——

Mr. STEARNS. So I could actually see it if I wanted to.

Ms. TOTH. Right.

Mr. STEARNS. And not just get your categories——

Ms. TOTH. We have a slide that shows our log files or a sample of what we collect in the log files. I don't think actually a consumer would engage with that in a way that would be meaningful for the consumer because it is a very technical expression of a user's interaction with us on the site so what we do in our interest-based advertising and the behavioral targeting systems that we use is to take those visits and categorize them based on the types of interaction. So if a user visits sports, they will have a score that indicates they visit sports. The actual log files themselves would probably not be useful for a consumer to engage with. It is a series of—it is actually quite difficult to explain in plain English what is in a log file.

Mr. STEARNS. OK, but the customer would have access to it is what you are saying if they wish to?

Ms. TOTH. Well, the customer—we don't actually make it available because there are no tools that actually generate log files in a way that would be easily accessible for consumers. What we give consumers is ready access to our privacy policy, educational links, opt out opportunities that are abundant across the site.

Ms. WONG. The demo that we did for you about our ads preference manager is an attempt to make that interface real which is demonstrating the interest categories that are assigned to a cookie in order to target advertising because I think Anne is correct that if a user won't read a privacy policy they are surely not going to read code.

Mr. STEARNS. OK. Mr. Chester, before you can answer that question also, what do you do with the bad actors? I mean we sit here and we pass a bill and we set up opt in and opt out procedures, and we have got Yahoo! and Google, but what are you going to do with the bad actors and how—is it possible that in addition to developing this legislation so that all 50 states have one set because each state now is developing a different one so there might be a need for us at the federal level to develop it so you don't have 50 states with 50 different privacies. So I guess my question is twofold. What do we do with the bad actors and is it a possibility that you could set up good housekeeping seals that everybody would say I am safe with this site, bingo, I can go into it and feel comfortable, and the bad actors wouldn't get it and then you could differentiate and say I am not going to fool with those.

Mr. CHESTER. I think if you passed legislative standards, right, that would be the base line. Everybody would know basically that they are protected. You now have a changed FTC potentially and hopefully you are going to reauthorize it soon. I mean the FTC has been hampered in going after the bad actors. It has been constrained from really looking as closely at this market as it should be and hasn't had the resources, and it has also been in conflict. There is now a new chairman there. There is a new director of consumer protection. They really want to move on this issue, and they could in fact be empowered to go after the bad actors in a much more vigorous way. Of course, we don't want to see state preemption consumer——

Mr. STEARNS. Now when I had hearings on this one of the problems we found is that there was no reciprocity between countries and you had the bad actors outside the United States. And so part and parcel of this is to develop legislation with other countries where you have reciprocity so you can go after corruption and fraud and there is that ability to do it. Otherwise, no one is going to comply with the federal bill and they will be in another country.

Mr. CHESTER. Well, I do think we are falling behind the Europeans. They are going to have a better privacy policy and build a whole new online commerce business that is privacy friendly while we are lagging because they are moving. The market is really being shaped, and this is something positive about the industry, we are creating this global interactive market. Yes, there are European companies, yes, there are Asian companies, but they in fact have created the standard and that is terrific. What happens here can

shape the rest of the world. As for profiles, you can see company after company says I have all this information about an individual consumer. I would hope that under the legislation that consumer could see all the detailed information that is being collected about them.

Mr. STEARNS. Mr. Cleland.

Mr. CLELAND. Yes. I think if Congress is serious about this you need to focus on the concept of deterrence. I mean if privacy violations or repeated violations are important there needs to be a significant penalty of whatever is appropriate but if legislation is passed and there is no deterrent and there is also no significant way of getting caught meaning independent audits of some type, it will not have teeth. It won't be meaningful and it won't be accountable. So if you are serious about this, you really need to be thinking about how do you take unaccountability, which is a problem across the Internet, not just with privacy, and try and address that and create more accountability. It is never going to be perfect but it is a key.

Mr. STEARNS. Mr. Chairman, if you will give me a little slack here, I just want to bring this last question, which really is also what we as legislators are grappling with, and that is the regulatory side versus the enforcement. Mr. Cleland talked about the enforcement, and we have two jurisdictions here. We have the FCC and the Federal Trade Commission, so I would like to just start to my left and just go down, and perhaps you could give us a feeling of how you think this bill should come together in terms of jurisdiction with the FCC and the Federal Trade Commission. Some people think, well, the FCC could be the enforcer and the FTC could be the regulator, but I would be curious if each one of you, if you don't mind, take a few moments, Mr. Chairman.

Mr. FELTEN. I would say this is closer to an FTC issue. I think it is fundamentally a consumer protection issue.

Mr. STEARNS. So both for regulatory and enforcement?

Mr. FELTEN. Yes.

Mr. STEARNS. OK.

Ms. TOTH. I would agree with Mr. Felten. We have worked for a very long time with the Federal Trade Commission on issues of consumer privacy online. We feel very comfortable and believe that they are well versed to address this issue.

Mr. STEARNS. Ms. Wong.

Ms. WONG. I have to say I feel a little bit out of my depth in terms of understanding the jurisdiction between federal agencies, but like Anne we have worked for quite a while with the FTC. My experience in watching them over the last 10 years is they brought very effective enforcement actions.

Mr. KELLY. I would say as well that we worked extensively with the FTC so far along this and they also have a great deal of expertise in the competition area, which is one of the things that is driving better technology throughout the industry in terms of providing users more transparency and more control over their data so the FTC has developed a great deal of expertise in this area.

Mr. CHESTER. I would like to see a joint task force because in fact the FCC will have expertise at the network level and particularly with cases with—inspection. There is a real role here for the

FCC but when it comes to the ad itself and the consumer experience itself it is the FTC.

Mr. STEARNS. Yes, because, you know, this is going to develop once you get broadband more. You are going to see voice over Internet. You are going to see everything over the Internet. And so all communication is going to be through that media and so I think the FCC has a part and parcel role.

Mr. CURRAN. I think I would echo that, a nod to the FTC, certainly in terms of our business model for cookie-related activity. The FTC for over a decade with its workshops on technology has been instrumental in raising awareness of the policy and technical issues and very much determinant in setting the direction for self-regulation. And as for other business models and other regulatory schemes, I wouldn't be able to speak to that.

Mr. STEARNS. OK. Mr. Cleland.

Mr. CLELAND. FTC is the lead in close coordination with the FCC. The only problem would be is if jurisdiction got in the way of passing—if you want to pass legislation. That would be the only tragedy.

Mr. STEARNS. Thank you.

Mr. BOUCHER. Thank you very much, Mr. Stearns. The gentleman from New York, Mr. Weiner, is recognized for 5 minutes.

Mr. WEINER. Thank you. Could I ask perhaps for Ms. Wong to talk a little bit about your experience developing Chrome, which is your—what is it called?

Ms. WONG. Browser.

Mr. WEINER. Your browser. Wouldn't it be possible through that vehicle so when you download it, your first page is tell us what information you would like to know about the pages you are visiting and what information that you would like to share, and maybe a collection of boxes you can check or not check. It is similar to kind of what Facebook tries to do although they don't do it right in your face. They kind of have you can say this—that seems to be an even better place to think about the true gateway to the experience. If I wanted to do that through Chrome, would I be able to do that in some way? I mean I know I can go and erase the cookies and I can erase my browser history, but can I do something like that?

Ms. WONG. Right. Thank you for that question.

Mr. WEINER. You are welcome.

Ms. WONG. And I am at a little bit of a disadvantage because I am not an engineer, just a lawyer, and our engineers do amazing things. I think that—I don't know if there is any limitation on what they can do. I know they are working very hard to build privacy controls——

Mr. WEINER. Well, perhaps if I could interrupt you maybe Mr. Felten can tell me about the technology possible here.

Mr. FELTEN. Sure. The information flows that users might be concerned about mostly happy not at the browser but after the user has interacted with a web site or a content provider, so what that means is that technical controls would exist mostly not in the browser but in the web sites themselves.

Mr. WEINER. Let me interrupt on that point. But if you have a fairly finite number of browsers that most people use, let us say for the purpose of this conversation it is 5. That basically probably

accounts for most of what people do. And the browsers are themselves competitive with one another. You can argue that the browser industry grew out of people's dissatisfaction with Explorer. So why couldn't you say that if you want your web site to come up when you traveling through Firefox, you have to have certain of your own information that you are giving us about what we can tell our users. Isn't that kind of a technical solution, a solution but a technical way to kind of serve as a gatekeeper for a lot of web sites?

Mr. FELTEN. Yes, and certainly there are things you could do along those lines so that the browser could help the user express their preferences and the browser could in a technical way query a site and see what promises the site makes about uses of data. There have been efforts to do this in the past. There was a standardization effort called P3P, the platform for privacy preferences, which defines such a standard and for reasons that are subject to debate the standard didn't stick. It wasn't popular. Nonetheless, I think this is a fruitful approach and I for one would be happy if the companies got together and had a discussion again about how to do this.

Mr. WEINER. Mr. Kelly, tell us a little bit, if you could, about your experiences in stepping on the toes of people's privacy concerns. It seems to me that we to some degree have three companies that have succeeded because consumers with a lot of different choices have chosen to use Google, chosen to use Yahoo, chosen in large numbers to go to Facebook. Could it be that the reason they are choosing your 3 services in particular is that you are being self-selected by an active consumer marketplace that thinks privacy works on your sites? You just had an experience, I guess it is an ongoing one, where you had kind of a conversation with your members about privacy. How does it work differently on yours than say—what search engine do you use when you are searching the Internet personally?

Mr. KELLY. It is usually Google.

Mr. WEINER. How is your privacy experience as a consumer of Google different than as a member of Facebook, is it at all?

Mr. KELLY. Well, I think that all three of these sites have succeeded because they are providing great user experiences overall, and in come cases those are around privacy, and because we have based a business on identity and personal information and the effective sharing of that with people who share a social context with you, we knew going in that privacy was going to be a critical issue for us. And our goal has been to build technologies that allow people to make choices, so one of the things that has gotten lost in the discussions of social networking is that friending, whether your friend somebody or not and how you connect to them is in and of itself a privacy setting. It determines what information that you see on Facebook, and that has been a great experience for us.

When you look at Google or Yahoo! as a search engine, they are looking to deliver a different experience there. They are looking for you type in a word or two and get back something that they think is the most relevant experience for you to get you to the page that you need to go next. If you use other services on those sites, they are providing different experiences there. Our goal has been to

build technology that empowers users and lets them make their own choices about how they share information. We have aimed to extend that into the advertising realm as well.

Mr. WEINER. Mr. Chester, I know you want to answer this question, but let me build on it. You can go ahead and in my last few seconds you can answer, but I take you back to 1986 or even 1996. I don't even know when this phenomenon all began. You could buy someone's credit report from three different companies. You could probably find aggregators of information that helped car dealers figure out who to send their information to. You could probably scrub public records to find out what kind of a home that they own, how much taxes they paid. It seems to me that there have always been resources that allowed someone to do 75 percent of what you described in your testimony as the thing we are protecting against. And we have acted here in Congress to try to limit access to that information but to some degree wouldn't you agree that consumers have pretty much now have a lot of tools that inform their experience.

I would argue without knowing, I bet you there are places I can go on the Internet to even find little software plug-ins I can probably download to let me know who is doing what and what web sites are good or bad at protecting information. So it is a two-part question. One is in a lot of the stuff that you are most concerned about is going to be out there whether you don't plug into the Internet at all, and, secondly, isn't some degree the marketplace allowing—aren't consumers allowing the winners to be the good privacy companies? So why don't you take both those——

Mr. CHESTER. Polls after polls after surveys including the one that UC Berkeley just released about a week ago, 10 days ago, say that the most users, most consumers, have no idea about what is being collected, how it is being used, how it really works. I honestly believe, and I think this is going to come out as part of this debate, and, frankly, that is why we need good privacy legislation because it is going to undermine public confidence. People don't really know what is going on inside Facebook and the third party developers and all the data flowing out. They don't know what Google is collecting across its various interests. If they knew, they would, in fact, I think be more concerned, so consumers don't know. The polls show that. This is a whole different world here than it was back in 1996 or 1998 when we did the children's act.

You are talking about the instantaneous merging of a vast number of offline databases with online behavior minute by minute that is adopted to an individual's actions and reactions with various online environments including all the personal information they put on their social networks. This is a completely different system that has been created. And, finally, you know, I have a 16-year-old. I look at this as the world that will be here very soon. We will be buying our mortgages on this mobile phone in the not too distance future. This is the dominant way we are going to be doing business for the PC and the mobile phone. It is a whole different world that has been created. On the one hand, we should be proud of it. They created it for us. We just have to make sure that consumers are protected.

Mr. WEINER. Thank you, Mr. Chairman.

Mr. BOUCHER. Thank you very much, Mr. Weiner. The gentleman from Louisiana, Mr. Scalise, is recognized for 5 minutes.

Mr. SCALISE. Thank you, Mr. Chairman. When we talk about opt in versus opt out, and I would imagine for business model purposes opt out is the preference because if you force somebody to opt in, I would think it would probably limit the number of people that would want their data to be collected on the front end, but if they do go through the process of opting out, are they actually stopping their personal data from being collected or are they just not getting the targeted advertising. If Ms. Toth could start.

Ms. TOTH. When a user is opting out for us that is an opt out of not collection but of use of the information, but I also want to be careful about the use of the term personal information because very often what is being conveyed to us is information that is specific only to a browser that is used to customize advertising. But even that level is what the user is able to opt out of in terms of that data being used.

Mr. SCALISE. But in different levels, of course. If you are just going on to a browser, and I think Ms. Wong talked about that, if I just go on to Google and do a search there is different information, maybe just my IP address, but then if I actually use Yahoo! for an e-mail account then clearly I am going to be giving you a whole lot more information and then you will have access to that, and if I choose to opt out of that what am I opting out of there? Are you not going to be collecting that data anymore or are you just not going to be giving the targeted advertising?

Ms. TOTH. The way that we do it at Yahoo! is that when a user opts out, we are no longer showing them targeted advertising, and we are not using their information in that particular way. Yahoo! offers a wide array of products and services, as you mentioned, e-mail, search, a wide array of different——

Mr. SCALISE. Maybe social network services.

Ms. TOTH. Social networking, exactly. So when a user opt out, we opt them out of the delivery of targeted advertising, but we also recognize that users may not want us to have that much information about them, so we take great pains to de-identify the data as soon as we can. We spent over a year looking at every single product, every single data system at Yahoo! to really try to minimize the amount of time that we hold data about users.

Mr. SCALISE. Right. I know we got limited time, so, Ms. Wong, and then Mr. Kelly.

Ms. WONG. Sure. I think it is roughly the same answer that I gave earlier, which is we really collect very little data from users when they are searching the IP address and the cookie, and the opt out for our interest-based advertising is an opt out for those targeted ads, and that it means is that the cookie you are getting is not uniquely identified. It just drops the query that you send us or the data that we have gotten into a bucket of all opt out cookies.

Mr. KELLY. Because our service is based on sharing personal information with others, we inevitably end up collecting a great deal of personal information so that we can effectively share it with others, and actually ask people to retain people's photo albums for them, which they usually expect to be retained indefinitely. In certain circumstances, and particularly in our advertising products,

where we are innovating and where people may not be used to a presentation in a particular way, we have allowed for opt outs in those instances because we think it empowers users. It allows them to say I am not comfortable with this at this point, but they can reconsider that at a later time. Our goal overall, and I think the goal of this committee and any legislation it considers and any enhancement of regulatory authority should be to make sure that consumers have real power to make those choices. We have tried to embody that in technology as much as we can, and you are here trying to embody it in law and trying to encourage the regulatory agencies to continue to meet their burdens and their obligations under existing law.

Mr. SCALISE. And I apologize to interrupt. I have only got a minute left. There is something else I want to ask especially as it relates to the e-mail services. And both for Yahoo! and Google, if you can answer this. If a user of Yahoo! or Google or any other e-mail service decides that they want to opt in or they don't opt out to all of those agreements, and you can collect whatever information you want from them, but let us say they then send me, and I don't have that service, and they send me an e-mail. I didn't agree to any of those issues. Do you read e-mails from people that are a Yahoo! or Google e-mail subscriber? Do you read through those e-mails to gather information in any way?

Ms. TOTH. Yahoo! does not scan the content of e-mail communications in order to share targeted advertising.

Mr. SCALISE. Or for any other purposes?

Ms. TOTH. We don't—well, there are only some purposes for—there is a process that actually removes viruses from e-mail that is an automated process but we don't use the content——

Mr. SCALISE. For advertising. Ms. Wong.

Ms. WONG. Yes. We are using that same technology that scans for viruses and also scans for spam. It is basically technology that looks for pattern in text, and we use that not only for the spam blocking and viruses but also to serve ads within the Gmail user's experience so importantly like the——

Mr. SCALISE. So if two people are exchanging an e-mail about a sporting event and they are talking about going to the game and then maybe they are going to want to go out for a drink afterwards, could they then maybe expect to get an advertisement about which different bars are offering specials after the game?

Ms. WONG. They won't get an e-mail with an advertisement but only the Gmail user will be able to see ads that shows up just like they show up on the side of our search results that are key to specific words—they are key words just as if you typed them into our browser that are calling from our repository of millions of ads to deliver an ad that is targeted to the content that you are reading.

Mr. SCALISE. So if that was a two-way conversation, one was the Gmail subscriber who agreed to or didn't opt out of the privacy but the other person in that conversation was not a Gmail user, clearly not someone who opted in or opted out, would any part—because in an e-mail thread they could have had maybe four or five replies and you got a long thread built up, and it is not just going to be the Gmail's information that is going to be there. The person who

is a non Gmail user is also going to be included in that thread. Would any of that information be read?

Ms. WONG. The non Gmail user will not have any ads targeted to them at all.

Mr. SCALISE. Is any of their data collected from that conversation?

Ms. WONG. Their data sits in the recipient's, the Gmail recipient's e-mail archive.

Mr. SCALISE. So if you have got algorithms that went through that Gmail e-mail, then when you were reading things in that e-mail some of the things that you were reading——

Ms. WONG. Were scanned.

Mr. SCALISE [continuing]. Would have been part of the thread of a non Gmail subscriber.

Ms. WONG. That is right.

Mr. SCALISE. How does your privacy policy handle that because that person clearly has absolutely no knowledge of you reading their e-mail, they surely didn't agree to it, and they didn't have the ability to opt out, so how is that handled?

Ms. WONG. Yes, just to be really clear. There are no humans reading e-mail at our company.

Mr. SCALISE. But even if it is a software algorithm that is trained to go through and look for key words or key information, their e-mail address, of course, is going to be in there, so you would be able to know who that person is at least from their e-mail address, but also you would be able to have access to the information. Do you have anything in those algorithms that prevents that information that is not Gmail related to be read from a person who didn't agree or have the ability to opt out of the privacy——

Ms. WONG. It would have to be that the user decided that they did not want to receive that e-mail from the person who sent it to them so this is fully in control of the Gmail account holder, and they can refuse to receive e-mails from certain people.

Mr. SCALISE. So you would be putting the burden now of privacy collection on a user of Gmail, someone who actually has a Gmail account?

Ms. WONG. So our user——

Mr. SCALISE. But your user actually knew what your policy was and could today right now go online as you showed, you got many opportunities for your users to opt out.

Ms. WONG. That is right.

Mr. SCALISE. The person who is the third party who is the non Gmail subscriber who is part of that thread does not have that same access so how can you put the burden on the person who sent the e-mail?

Ms. WONG. No, no, no. The person who sent the e-mail has—they have sent their e-mail to their friend. That user is not going to get any ad targeted to them. We are not going to have any information about that user at all.

Mr. SCALISE. Is any of their information read?

Ms. WONG. Except for the fact that we hold their e-mail because we are the e-mail service provider for the Gmail account holder, which is the same as any other web mail service.

Mr. SCALISE. I guess the real question is how is that person—the Gmail subscriber clearly has the ability to protect their privacy, to opt out if they so choose. Maybe some of their data is still collected but they could still opt out but the third party that they sent the e-mail to who then replied back to them who is contained in that thread doesn't have that same ability but their data is subject to being searched in the same way, so how——

Ms. WONG. That is true, but that occurs with every web mail service because every web mail service——

Mr. SCALISE. But Yahoo! just said that they don't do the same thing.

Ms. WONG [continuing]. Scans their e-mail.

Mr. SCALISE. I will ask Ms. Toth if that——

Ms. WONG. Every web mail service scans their e-mail for spam, scans it for viruses. It is the same process.

Mr. SCALISE. But also for targeted advertising, I think you said you all do scan it for targeted advertisements. Ms. Toth said they do not.

Ms. TOTH. We do not target. We don't——

Mr. SCALISE. And I guess in the case where they are scanning it for other services that would be maybe sold to a third party, how does the person protect their privacy when they never had the same opportunity to opt out that the original Gmail subscriber who sent the e-mail was able to have the same access?

Ms. WONG. To be very clear, no user's information is sold to any third party. No information about the sender of an e-mail to a Gmail account is——

Mr. SCALISE. But if——

Mr. BOUCHER. Mr. Scalise, you are now past 10 minutes of time. We are going to wrap up.

Mr. SCALISE. If I can get that in writing maybe the answer to that. Thank you.

Mr. BOUCHER. That is fine. If any of the witnesses would like to respond to that last question in writing, that would be highly appropriate. The gentleman from Vermont is recognized next, Mr. Welch, for 5 minutes.

Mr. WELCH. Thank you, Mr. Chairman. Thank you. I want to join my colleagues in apologizing for the delay and appreciation for your patience although I think I might rather have your job today than ours. Ms. Wong, in your written testimony you noted that the committee should continue our efforts to explore the privacy issues. This is obviously an incredibly difficult issue, both because of the complexity of making this work and assuring confidence to users and because of basic questions about what should be private and what isn't. I am asking that you expand on that and what ongoing efforts is Google making about the merging of online and offline data and the issues that are created as a result of that. I would start by asking you if you would comment on that and probably ask a few others as well.

Ms. WONG. Sure. And I actually think this is a multi-dimensional question. I think absolutely there is an obligation on industry to do the right thing because the trust of our users is incredibly important. I also think that there is a role for groups like Mr. Curran's group, the self-regulatory groups, which continue having us inno-

vate on best practices. I think the best thing that has happened in the last few years that all of the major Internet companies are competing to create better privacy technologies, and that is really phenomenal. There is also a role for government because to be very clear, there are bad actors, and so there is a role for oversight into the range of players on ecosystem and the conduct that they engage in.

And the thing that I think is most important, and the reason it should apply to both online and offline is that the companies that you have here all face our users, are all invested in deepening the relationship with our users. There are companies that do not face the public that are behind it and that need more oversight because nobody knows what they do with their data.

Mr. WELCH. Mr. Curran, do you want to comment or anything else to add? Kudos to you for the role that you play.

Mr. CURRAN. I would simply say I think we have an obligation to tell you about our successes and areas of improvement as self-regulatory organizations as it relates to—and also to, I think, work with you to explain the somewhat complicated technologies that go around the different business models. I don't believe that—I have diverse memberships that we are not in the position of having a legislative view at this time, but we are very much committed to educating the committee on the technologies, and I think today's hearing has been very helpful on that in terms of in effect helping you discern the exact technical infrastructure that goes into all of this online advertising.

Mr. WELCH. Well, let me come back to Mr. Kelly. The Congress is never going to be able, obviously, to address technical issues. It is not our competence. It is not our job. It is not what we should do. What specific things in terms of policies, I will ask you, Mr. Kelly, what would you be recommending that Congress do in order to protect privacy, which is our proper concern, but do it in a way that doesn't strangle innovation?

Mr. KELLY. And that is a critical role that you do have is to protect the innovation in American technology and how we have been able to lead the world in this area. But, obviously, protecting the privacy of American consumers is critical to us and to other companies in the technology industry but not everyone. And so there are many actors out there who are tasked and see their role as gathering data and building personal profiles of people with no notice, no consent, no control. I think that Congress' regulatory action should be largely directed there. We have a set of existing and extensive regulations, and we have talked tonight about our work with the FTC as a technology industry in this area where there are bans against deceptive practices and other activities, but still there are many technology companies out there, whether they be spyware vendors, whether they be sort of just surreptitious collectors and aggregators of personal data that deserve the attention of this committee, the Congress, and existing regulators.

Mr. WELCH. Thank you. My time is almost expired and I yield the balance of my time.

Mr. CLELAND. Could I answer?

Mr. WELCH. It is up to the chairman. I think I am almost out of time.

Mr. BOUCHER. Yes, that is fine. Go ahead, Mr. Cleland.

Mr. CLELAND. Yes. I think the key concept of what you are looking for that the FTC and others should build on is longstanding, fair representation law. We obviously have a huge gap. Jeff mentioned a lot of the polls out there. Consumer don't have a clue about all the stuff that is being collected on them, not a clue. And so if you believe in fair representation and you take the facts of all the people that have been dealt with on the Internet and they don't know what is going on, there is a serious breakdown in fair representation.

Mr. CHESTER. Do you think I could add something?

Mr. BOUCHER. Mr. Chester, please.

Mr. CHESTER. Just very briefly. All the companies here, including the members of NAI, as far as I can see, are increasing the amount of data they are collecting on consumers. It is not that there is a question of best practices. They are building and expanding the data collection. That is the nature of the business. That is the nature of the online advertising system to build out these very sophisticated approaches. Therefore, you need to have rules, you need to bring PIA up to date, because you don't need to know your name anymore to know who you are. You need to protect sensitive data and you have to have the FTC be a better watchdog.

Mr. BOUCHER. With that, Mr. Welch, your time has expired. And let me say thank you once again to our witnesses for what truly has been an informative session. Long delayed, but well worth our time talking to you, and we thank you very much for taking your time, all day, in fact, to talk to us. I have clearance for unanimous consent from the minority to place in the record a letter to the subcommittee, the joint subcommittees actually, from the Federal Trade Commission, concerning the subject of today's hearing, a letter from Data Foundry, a data company based in Austin, Texas. Without objection, those will be made a part of the record.

[The information appears at the conclusion of the hearing.]

Mr. BOUCHER. And without objection, the record of this proceeding will be kept open for a period of 3 weeks so that other members of the subcommittee can submit to our witnesses questions in writing. And as you receive those questions from the members, if you could respond to them promptly, that would be much appreciated. Thanks again to you for an excellent hearing. This hearing stands adjourned.

[Whereupon, at 8:20 p.m., the subcommittees were adjourned.]

[Material submitted for inclusion in the record follows:]

Statement of
Representative John D. Dingell
Committee on Energy and Commerce
Subcommittee on Commerce, Trade, and Consumer Protection
Subcommittee on Communications, Technology, and the Internet
Hearing on "Behavioral Advertising: Industry Practices and Consumers' Expectations"

June 18, 2009

Thank you, Mr. Chairman. As we commence the Committee's investigation of behavioral advertising, I feel it prudent that we do so in a comprehensive and objective manner. Much controversy and opinion surround this issue, and in the notable absence of specific Federal statute governing this manner of advertising, we are behooved to proceed in such a way that establishes a thorough record, which, in turn, will allow us to write fair and adequate legislation.

Regarding our discussion about behavioral advertising today, I suggest we examine several key issues. First, and perhaps most practically, what Federal agency or agencies will be tasked with

enforcing data privacy laws as they pertain to behavioral advertising? I would note that provisions of the Communications Act, specifically section 631, and the Electronic Communications Protection Act (ECPA) seem to be applicable to the sharing of consumer information among Web sites, Internet service providers, and online content providers for the purpose of behaviorally-based advertising. These two statutes are administered by the Federal Communications Commission and the Department of Justice. All the same, we are concerned primarily with consumer protection, something with which the Federal Trade Commission is tasked.

Second, we must seek to find balance between the needs of consumers and businesses as they relate to behavioral advertising. On the one hand, consumers have a right to transparent and comprehensible online privacy policies. On the other, many online businesses, such as newspapers and Web sites, depend upon behavioral advertising for much, if not all, of their revenue. At a time of recession, dealing a crippling blow to these businesses via

overly strict advertising laws may distort the functioning of the Internet as we currently know it, thus arguably harming consumers, and also do little to aid sorely needed economic growth.

Third, and though perhaps on a note more ancillary to behavioral advertising, I believe our broader discussion of data privacy should extend beyond the Internet to physical records. Although identity theft is commonly discussion in connection to the Internet, paper-based records also provide bad actors with ample fodder for all manner of unsavory activity harmful to consumers.

All of this in mind, I wish you every success in this valuable hearing, Mr. Chairman, and hope to be of some service as the Committee moves forward with legislation. I thank you for your courtesy and yield back the balance of my time.

Statement of
U.S. Representative Edward J. Markey (D-MA)
Subcommittee on Communications, Technology
And the Internet
Hearing on Electronic Privacy
June 18, 2009

Good Morning. I'd like to commend Chairman Boucher and Chairman Rush for calling this joint hearing today. As members of the Committee well know, I have a longstanding interest in privacy issues, and along with the Ranking Member of the Full Committee, Mr. Barton, I am co-chair of the Privacy Caucus.

Today's hearing will allow us to explore the many issues involving electronic privacy, particularly the rise of behavioral marketing.

Like many, I was concerned last year and held hearings around so-called "deep packet inspection" technologies that were being implemented and planned in ways that undermined consumer privacy. Obviously, broadband providers are in a position to know virtually everything about a person's Internet use and ensuring that such providers uphold very high privacy standards and avoid the collection of sensitive personal information and safeguard that which is legitimately collected is vital. In addition, many online companies are in a position to also know significant amounts of potentially sensitive personal information about users. For these reasons, I have long advocated that Congress should enact a "Privacy Bill of Rights" for the digital era to ensure that consumers are fully protected in their online experience and that trust exists in commercial interactions.

There are many provisions that ought to be considered in any such legislation. I am very interested in expanding a privacy

provision that I successfully enacted to protect wireless location information. That provision prohibits wireless carriers from using wireless location information for commercial purposes without the express prior consent of the subscriber. However, for germaneness reasons, the provision could not extend at the time I offered the amendment to 3rd party application providers not regulated by the Federal Communications Commission. I believe we need a consistent policy in this area. In addition, as the author of the Child Online Privacy law, I question whether any behavioral marketing should be permitted for the online activities of children. This strikes me as highly inappropriate and I would like to explore ways in which we can provide greater protection to children in this area.

Again, I commend the Chairmen for this hearing and look forward to working with them and our other Committee colleagues as we move forward. Thank you. ####

Statement of Congresswoman Anna G. Eshoo
Hearing on Behavioral Advertising: Industry Practices and Consumers' Expectations
Subcommittee on Communications, Technology and the Internet
June 18, 2009

Thank you Mr. Chairman and welcome to the witnesses.

This is an important hearing and I'm so pleased that some of the most important players on the Internet are here today. I'm also pleased to welcome them as my constituents.

I'm eager to hear from the witnesses but I would like to note that one thing is apparent at the outset – not every 'Internet' company has the same business and Internet users have different relationships and provide different information to each part of the Internet 'stack'.

On one end of the Net there are ISPs, who send someone to your house to drill holes in your walls, provide you with a modem, ask you to sign a service contract and then send you a bill every month.

At the other end are a wide range of websites and web services which Internet users actively engage to make purchases, view content, and utilize online tools. Frequently, consumers voluntarily provide personal information to these sites, but often they are completely anonymous.

In between are a number of advertising servers, data aggregators, security monitors, and other companies that operate beyond the view or knowledge of the typical web user.

In addition to this are a host of devices – personal computers, iPods, mobile phones – that consumers use in conjunction with the Internet and that can have associated software that provides data back-and-forth to the manufacturer.

Each of these layers of Internet businesses has a different relationship with web users and they have different access to information about the user, their interests or their web surfing habits. And I believe any comprehensive privacy framework should regulate each of these businesses within a structure that recognizes these differences and responds to the disparate business models and customer relationships involved.

Let me be clear – I support a new privacy framework to protect the privacy and security of Internet users. I do not support a 'one-size-fits-all' policy that puts personal computer manufacturers, website operators, Internet service providers, and advertising serving companies all in the same 'regulatory boat'.

This makes no sense as a policy and would have a counterproductive impact on consumer privacy and on their Internet experience.

Thank you Mr. Chairman and I look forward to the witnesses' testimony.

Office of the Secretary

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

June 16, 2009

The Honorable Bobby Rush
Chairman
The Honorable George Radanovich
Ranking Member
Subcommittee on Commerce, Trade,
and Consumer Protection
Committee on Energy and Commerce
United States House of Representatives
Washington, D.C. 20515

The Honorable Rick Boucher
Chairman
The Honorable Cliff Stearns
Ranking Member
Subcommittee on Communications,
Technology, and the Internet
Committee on Energy and Commerce
United States House of Representatives
Washington, D.C. 20515

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

Thank you for the opportunity to share the views of the Federal Trade Commission ("FTC" or "Commission") regarding online behavioral advertising – the practice of collecting information about an individual's online activities in order to serve advertisements tailored to that individual's interests. The Commission applauds your attention to this topic and looks forward to assisting the Committee in any way we can. The Commission has actively encouraged industry to embrace new measures relating to behavioral advertising to inform and empower consumers and is monitoring developments, both in this space and more broadly, to ensure that consumers' privacy is protected.

As you may know, the Commission has been concerned about the privacy issues related to behavioral advertising for some time. Indeed, our work in this area dates back to 1999, when the FTC held a joint public workshop with the Department of Commerce on the practice, then called "online profiling."[1] A copy of the report summarizing the Commission's efforts in this area – *FTC Staff Report: Self Regulatory Principles for Online Behavioral Advertising* ("Staff Report") – is enclosed.[2]

---

[1] FTC and Department of Commerce Workshop, *Online Profiling Public Workshop* (Nov. 8, 1999), *available at* http://www.ftc.gov/bcp/workshops/profiling/index.shtm.

[2] The report was published on Feb. 12, 2009 and also is available at http://www2.ftc.gov/os/2009/02/P085400behavadreport.pdf.

In recent years, the FTC has increased its efforts in this area. More specifically, in November 2007, the Commission held a two-day public "Town Hall" meeting that brought together various stakeholders to discuss online behavioral advertising.[3] As the presentations and discussions at the Town Hall made clear, the privacy issues surrounding the practice are challenging. Although behavioral advertising may provide benefits to consumers in the form of free content and a more personalized online experience, it also raises significant privacy concerns. Adding to the complexity is the fact that the business models are diverse and constantly evolving.

In November 2008, to address the privacy concerns raised by behavioral advertising, Commission staff released for public comment a set of proposed principles (the "Principles") intended to encourage and guide industry efforts to develop guidelines governing the practice.[4] The Principles call for increased transparency and consumer control, reasonable security, and affirmative express consumer consent when a company collects and uses sensitive information or makes material changes to its privacy promises. In February of this year, the Commission issued the attached Staff Report analyzing the public comments received, setting forth additional guidance regarding the Principles' scope and implementation, and discussing efforts to date by industry and consumer groups to address the privacy concerns in this area. Concluding that significant work still was needed to address these concerns, the Staff Report called upon industry to redouble its efforts to develop self-regulatory programs, and to ensure that such programs included meaningful enforcement.

Since then, a number of individual companies have taken steps to improve their practices. For example, some companies have developed new means for notifying consumers when their data is collected for behavioral advertising, new tools to allow consumers to permanently opt out of the practice,[5] and features allowing consumers to manage and control their online marketing profiles. Additionally, some search engines allow consumers to search the Internet anonymously, and a number of companies have reduced the amount of time they retain consumers' data.

Trade organizations also are in the process of revising their codes of conduct, or creating new guidelines, in order to ensure that their members' practices are consistent with the Principles. Further, one newly-created think tank composed of industry members, academics, and advocacy groups, has begun systematically to examine the best ways to provide transparency

---

[3] FTC Town Hall, *Ehavioral Advertising: Tracking, Targeting, & Technology* (Nov. 1-2, 2007), *available at* http://www.ftc.gov/bcp/workshops/ehavioral/index.shtml.

[4] FTC Staff, *Online Behavioral Advertising: Moving the Discussion Forward to Possible Self-Regulatory Principles* (Dec. 20, 2007), *available at* http://www.ftc.gov/os/2007/12/P859900stmt.pdf.

[5] Such "persistent" opt-out tools are important, as they allow consumers to delete tracking cookies from their computer's browser without also deleting the cookie that records the consumer's decision to opt out of behavioral advertising.

and consumer control in the behavioral advertising space.

The Commission is encouraged by these developments, and will continue to monitor the marketplace to ensure that they continue. Commission staff also will continue to investigate specific practices to determine whether they violate Section 5 of the FTC Act or other laws. For example, the FTC recently announced a proposed settlement with Sears Holding Management Corporation resolving allegations that the company failed to disclose adequately that it was collecting detailed consumer data, including information about consumers' online browsing activity, through tracking software.[6] In addition, staff will continue to meet with companies, consumer groups, trade associations, and other stakeholders to keep pace with changes, and will look for opportunities to use the Commission's research tools to study developments in this area.

The Commission appreciates this opportunity to submit its Report to the Committee and looks forward to working with the Congress on the issues related to online behavioral advertising.

By direction of the Commission.

Donald S. Clark
Secretary

Enclosure

[6] *In the Matter of Sears Holdings Management Corp.*, FTC File No. 082-3099 (June 3, 2009 proposed consent order and complaint), *available at* http://www2.ftc.gov/os/caselist/0823099/090604searsagreement.pdf.

PRINCETON UNIVERSITY

Edward W. Felten
Professor of Computer Science and Public Affairs
Director, Center for Information Technology Policy

Sherrerd Hall, Room 302
Princeton, New Jersey 08544
T 609.258.5906 F 609.964.1855
E felten@cs.princeton.edu

July 28, 2009

Hon. Henry A. Waxman
Chairman, House Committee on Energy and Commerce
2125 Rayburn House Office Building
Washington DC 20515-6115

Dear Chairman Waxman:

Thank you again for the opportunity to testify at the joint hearing on "Behavioral Advertising: Industry Practices and Consumers' Expectations". I am happy to respond to the Questions for the Record submitted by Congressman Radanovich, as conveyed by your letter of July 14, 2009. My responses are attached. I would be happy to answer further questions from the Committee or staff at any time.

Sincerely,

Edward W. Felten

Responses to Questions from Hon. George Radanovich

Question 1: How does an ad service discover the real-world identity of an online user?

An ad service could discover a user's real-world identity by piecing together information about the user from different sources. In some cases, the user will reveal his real-world identity, or information sufficient to deduce his identity, to a website he uses. For example, he might reveal his name, hometown, and date of birth to a social network site, or he might use a site to engage in a financial transaction revealing payment information that can be linked to identity. In such cases, the site can convey identifying information to the ad service—or in some cases the site may be run by the same company as the ad service. Given enough information to identify a user uniquely, the ad service can then consult commercially available consumer databases to learn more about the user.

Even if the user does not convey identifying information to a single site, an ad service that places ads on multiple sites will be able to connect the dots between the user's visits to those sites, so the service will know that it can aggregate information about the user that it gets from all of the sites. If one site learns a user's name, another learns his date of birth, and a third learns his hometown, the ad service could piece this information together to identify him.

In addition to information the user provides explicitly to websites, some information can be gathered directly by the ad service, in the course of providing ads to a user. This includes the user's IP address, which the Internet uses to route traffic to the user. IP addresses can often be traced to a particular organization or to a geographic location ("geolocation"), with the help of commercially available services. For example, my laptop computer often connects to the Internet on weekdays using an IP address that can be traced to Princeton University, and the same laptop often connects on evenings and weekends using an IP address that can be geolocated to the town of Princeton, NJ. From this, an ad service might deduce that I work at Princeton University and live in the town of Princeton—information that could be useful in identifying me.

Question 2: If an ad service buys a consumer information database that has additional information such as credit history, can more ads be directed at consumers who are known to be more frequent shoppers?

Yes. An ad service can direct more ads, or more ads of a certain type, at individual consumers based on any information the ad service has about the consumer. Ad services can direct more ads at consumers who are more frequent shoppers.

Question 3: Your written testimony described a "web bug" as a clear picture loaded on a webpage by an ad server that is not apparent to the consumer.

a. *What information can a "web bug" collect and send back to the ad server that placed the "web bug?"*

b. *Do "web bugs" challenge the ability of consumers to avoid being tracked?*

c. *How can they be avoided?*

A web bug is very similar to an ad; the only difference is that an ad displays some visible content to the user, while a web bug is invisible. A web bug might be implemented as a tiny, transparent image on a page, although other implementations are possible.

(a) Because a web bug is so similar technically to an ad, a web bug can gather, and send back to an ad server, exactly the same information that an ad can gather and send.

(b) From a consumer's standpoint, web bugs differ from ads only in that ads are more evident. A savvy consumer might see an ad on a webpage and assume that he is likely being tracked by an ad service. Because web bugs are not visible, a consumer might look at a page containing web bugs but no ads, and conclude wrongly that nothing on the page was tracking him. In principle, a very savvy consumer with technical skills could examine the source code of the webpage and detect the web bug, but very few consumers will have the skills and time to do this. To the extent that consumers try to thwart tracking by behaving differently when they see ads, their strategy will fail if invisible web bugs are being used for tracking.

(c) If consumers want to protect themselves against being tracked by web bugs, they can use the same methods they would use to protect themselves against tracking by ad services. These methods include market mechanisms, such as avoiding websites that do not credibly promise not to use web bugs; technical countermeasures against tracking, such as browser facilities that control third-party cookies; and ad-blocking technologies. Ad-blocking technologies may be the most effective countermeasure against web bugs, but if too many consumers adopt ad-blocking, the economic viability of ad-supported content may be put at risk.

Question 4: Although the industry continually tries to improve privacy policy notices to make them more user-friendly, such notices remain long and complicated legal documents. Is there utility in trying to create a "nutrition label" type approach—a uniform and easily recognized notice—so consumers can "comparison shop"?

"Nutrition labels" for privacy are a promising idea. As with food labeling, a simple, standardized label can help consumers make good decisions. This is an idea that deserves more attention.

The challenge lies in how to boil down long, complex privacy policies into a concise set of categories that are easy to understand and can be presented in a simple display. The standard nutrition labels on food essentially convey seventeen numbers. By contrast, the best proposed "nutrition label" for privacy uses a grid of 70 boxes, with each box containing one of four cryptic graphics. (See Kelley et al., *A "Nutrition Label" for Privacy*, available at http://cups.cs.cmu.edu/soups/2009/proceedings/a4-kelley.pdf.) Even this is substantial progress, but more work is needed to design even simpler labels and test their usability.

Government can help move us toward a viable privacy nutrition label by supporting further studies, convening dialogues involving industry and the other stakeholders, encouraging the development of consensus standards, and beginning to contemplate whether and how regulation might be advisable should a reasonable, widely-adopted consensus standard fail to arise.

YAHOO!

July 28, 2009

The Honorable George Radanovich
Ranking Member, Subcommittee on Commerce, Trade and Consumer Protection
House Committee on Energy and Commerce
2125 Rayburn House Office Building
Washington, DC 20515-6115

Dear Ranking Member Radanovich,

Thank you for the opportunity to follow up with additional information responding to questions you have posed in connection with the June 18, 2009 hearing entitled "Behavioral Advertising: Industry Practices and Consumer Expectations". Given the work Yahoo! has done in this area, it is a pleasure to provide a more complete picture to the committee for the record.

1. **Your written testimony stated Yahoo! is working on ways to explain interest-based advertising and related privacy notices to the consumer at the time of ad delivery. Please expand on how this would work.**

   Yahoo! has a long history of working to bring additional information to the user, as evidenced by the "Ad Choice" program we have run in conjunction with eBay's advertising since 2007. Yahoo! has been the exclusive company serving display advertising to ebay.com. When we serve the ads, we have joined with eBay to surface additional information to users from the frame of the advertisement as seen in Attachment A. Yahoo! and eBay have been able to do this because Yahoo! serves all ads to the eBay site, giving the user a consistent advertising experience. While we are proud of this effort, it has been challenging to find a way to duplicate this experience on sites where multiple ad networks may be serving the advertising. Yahoo! has worked out customized transparency solutions like this with various publishers where we serve ads exclusively, but this solution has not been scalable, meaning it would not work across a multitude of sites.

   Therefore, Yahoo! has been working with the Network Advertising Initiative (NAI) to develop a method of transferring "metadata", or flagged data sent along with an "ad call", which is the request for the advertisement sent from the website a user is viewing to the ad network or ad serving company responsible to serve the advertisement. I have attached Attachment B, which indicates the idea behind the effort, the data elements that we suggest be sent with the ad call, and some examples of ways the metadata could be displayed by the publisher's website on which the ad appears. We are also in the process of beta-testing this idea at http://green.yahoo.com/living-green/. A click on "Ad Info" just above the advertisement will surface the serving information to users.

   This idea is reflected in the self-regulatory principles recently released by the American Association of Advertising Agencies (4A's), the Association of National Advertisers (ANA), the Direct Marketing Association (DMA), and the Interactive Advertising Bureau (IAB) among others.

Yahoo! is now working with these organizations and others like the NAI and TRUSTe on various aspects of this idea to bring the principles to the implementation stage. We have started with the aim of getting a large swath of industry to adopt a standard for sending the metadata, and perhaps this will also result in an additional set of standards around how this information could be displayed to users.

2. **Although the industry continually tries to improve privacy policy notices to make them more user -friendly, such notices remain long and complicated legal documents. Is there utility in trying to create a "nutrition label" type approach – a uniform and easily recognized notice – so consumers can "comparison shop"?**

Yahoo! revamped its privacy policy in 2008 to enable users to more quickly find specific information about the products they use among our numerous offerings. The overall fundamentals of disclosure remain the same, but more specific or detailed information is also provided by product name. Yahoo! has also included information of special topics to help users understand the technologies behind online advertising and content delivery. We believe this "layered" approach gives users easy navigation tools to find significant amounts of information about the services they want to use. In addition, we make our opt-out very prominent and easily accessible from the first page a user sees when coming to the privacy policy. Yahoo! has also included information about third parties present on yahoo.com so that users can also go straight to their privacy policies to learn their practices as well.

The nutrition label concept for privacy policies has been explored for many years, and what has become clear is that there are not only a myriad of business models but countless device interfaces as well. This lack of uniformity in what is being provided by the many companies in the Internet space makes a standard labeling requirement impossible to implement.

Nonetheless, we do believe that information about all of the players involved in serving an ad *at the time the ad is served* may be very helpful to interested users. To that end, Yahoo! has taken steps in partnership with others in industry to develop the metadata proposal mentioned above. The implementation of such a proposal will give users first-hand information about the companies involved in ad serving and could offer the user an opt-out from the use of their information for interest-based advertising. Since the advertiser, the ad delivery company and the customization company may be different entities, we believe this is the critical information needed by most users related to interest-based advertising, and is a nutritional label of sorts.

3. **What information does Yahoo! collect?**

Yahoo! describes the information we collect in our privacy center at http://privacy.yahoo.com. Our policy reads:

Yahoo! collects personal information when you register with Yahoo!, when you use Yahoo! products or services, when you visit Yahoo! pages or the pages of certain Yahoo! partners, and when you enter promotions or sweepstakes. Yahoo! may combine information about you that we have with information we obtain from business partners or other companies.

When you register we ask for information such as your name, email address, birth date, gender, ZIP code, occupation, industry, and personal interests. For some financial products and services we might also ask for your address, Social Security number, and information about your assets. When you register with Yahoo! and sign in to our services, you are not anonymous to us.

Yahoo! collects information about your transactions with us and with some of our business partners, including information about your use of financial products and services that we offer.

Yahoo! automatically receives and records information from your computer and browser, including your IP address, Yahoo! cookie information, software and hardware attributes, and the page you request.

a. How does Yahoo! use the information it collects?

In the context of interest-based advertising, Yahoo! uses data to customize the advertising and content seen by a user, fulfill user requests for products and services, improve products and services, protect consumers and advertisers from fraud, bill advertisers for ads displayed or clicked upon, contact users, conduct research, preserve security, meet legal and reporting obligations and provide anonymous reporting for internal and external clients.

b. How long does Yahoo! keep the information it collects?

This question addresses what we believe is one of the most important elements in how companies protect user information. Yahoo!'s front-end/back-end approach, described in my testimony, outlines our view that in order to protect user privacy, users should be offered choices on the front end coupled with the commitment by companies to handle data responsibly through security and minimal data retention. Therefore, in December 2008 Yahoo! announced a data retention policy committing to anonymize server log data — including page views, page clicks, ad views, ad clicks, and searches — after 90 days. Server log data that is routed to systems Yahoo! uses to help prevent fraud and preserve security will be retained for up to 6 months – but only for that purpose. Yahoo! also must retain data longer in some instances to comply with legal obligations. This was both a dramatic reduction in the period of time log file data is kept in identifiable form as well as a significant expansion in scope from the original policy that applied only to search log data at 13 months. This policy will be fully implemented on a global basis by mid 2010.

There are a few exceptions where the data is needed to help us protect consumers and Yahoo! such as:

- Fraud and Security: To help protect our users and advertisers, Yahoo! will retain log data that is used to help detect and defend against fraudulent activity and preserve system security for up to 6 months. Employee access to this information is limited to this purpose.
- Legal: Yahoo! must comply with applicable laws and legal obligations that may require that Yahoo! retain log data for longer periods.

- User generated content and user registration data that is under the control of the user. Yahoo! users have the ability to modify or delete content such as emails, IMs, pictures, photos, and comments per the policies of the particular products.

c. With whom does Yahoo! share the data it collects?

The following information is Yahoo!'s current sharing policies and practices are in our privacy policy which can be found at http://info.yahoo.com/privacy/us/yahoo/details.html#3. The policy states:

INFORMATION SHARING AND DISCLOSURE

Yahoo! does not rent, sell, or share personal information about you with other people or non-affiliated companies except to provide products or services you've requested, when we have your permission, or under the following circumstances:

- We provide the information to trusted partners who work on behalf of or with Yahoo! under confidentiality agreements. These companies may use your personal information to help Yahoo! communicate with you about offers from Yahoo! and our marketing partners. However, these companies do not have any independent right to share this information.
- We have a parent's permission to share the information if the user is a child under age 13. Parents have the option of allowing Yahoo! to collect and use their child's information without consenting to Yahoo! sharing of this information with people and companies who may use this information for their own purposes.
- We respond to subpoenas, court orders, or legal process, or to establish or exercise our legal rights or defend against legal claims.
- We believe it is necessary to share information in order to investigate, prevent, or take action regarding illegal activities, suspected fraud, situations involving potential threats to the physical safety of any person, violations of Yahoo!'s terms of use, or as otherwise required by law.
- We transfer information about you if Yahoo! is acquired by or merged with another company. In this event, Yahoo! will notify you before information about you is transferred and becomes subject to a different privacy policy.

Yahoo! displays targeted advertisements based on personal information. Advertisers (including ad serving companies) may assume that people who interact with, view, or click targeted ads meet the targeting criteria—for example, women ages 18-24 from a particular geographic area.

- Yahoo! does not provide any personal information to the advertiser when you interact with or view a targeted ad. However, by interacting with or viewing an ad you are consenting to the possibility that the advertiser will make the assumption that you meet the targeting criteria used to display the ad.
- Yahoo! advertisers include financial service providers (such as banks, insurance agents, stock brokers and mortgage lenders) and non-financial companies (such as stores, airlines, and software companies).

Yahoo! works with vendors, partners, advertisers, and other service providers in different industries and categories of business. For more information regarding providers of products or services that you've requested please read our detailed reference links.

d. How does Yahoo! "anonymize" the data collected and after what period of time does Yahoo! "anonymize" the information?

Yahoo! uses a four step process to "anonymize" or "de-identify" the web log data within 90 days with the limited exceptions noted. The process is explained more thoroughly in Attachment C.

e. How does Yahoo! ensure that it shares only the minimum amount of information necessary for its purposes?

Yahoo! endeavors to collect, use and share information to provide our relevant services in a manner consistent with users' expectations of privacy. In the context of interest-based advertising, we collect information about users' online activities in order to offer them content and advertising they will find compelling. In the delivery of all of our services, Yahoo! adheres to internal policies such as the sharing and disclosure policy listed above as well as contractual obligations with vendors or partners around data usage. Finally, an important aspect of our data management policy is our effort to limit the amount of time data is held in identifiable form -- our data retention policy -- further limiting any potential risk to users.

f. What exactly can a user opt-out of?

Yahoo! is clear with our users that they can opt out of interest-matched advertising. This opt-out is prominent when a user clicks on the privacy policy link present on nearly every page of our network. The full text available to users to explain the opt-out and the persistence features offered is at http://info.yahoo.com/privacy/us/yahoo/opt_out/targeting/details.html.

g. How would a full opt-in versus a full opt-out regime impact Yahoo!'s business?

Yahoo! is fundamentally a service based on relevancy and customization. Our users value our services because we offer them relevant products and advertising and our business partners work with Yahoo! because we help them reach the customers who find their products and services of value. This exchange is built on a model of offering consumers a meaningful opt-out choice as we use their information to determine their needs. Altering the model to require each user to ask specifically for what they want – or to opt in – would fundamentally alter our service for consumers and business partners alike. Moving away from an opt-out regime could affect Yahoo!'s business in two key ways.

First, Yahoo! provides many highly innovative services for free to our users. We have built a massive, highly engaged audience by providing free, highly personalized products. Our

ability to invest in innovation depends on our ability to generate advertising revenue. Policies which could limit our ability to generate revenue from highly relevant, interest-based advertising could, in turn, limit the resources which we can invest in technological innovation.

Under an opt-in regime, the business model that allows Yahoo! to maintain such a vast array of industry leading, free products and services including finance, sports, news, personalized home page, mail, shopping, travel, etc. could be significantly undermined. Yahoo! would likely have to shutter some of these services, delay or suspend product improvements, or cease introduction of new innovative services. Many of our products are multi-award winners and are updated with new features and functions regularly. Other services to our users such as anti-spyware software, unlimited mail storage and generous photo and video storage are also provided for free because of the existing opt-out advertising model.

Second, interest-based advertising is a fast-growing part of our business because these ads perform better than non-targeted ads – they are simply more relevant for users, so those users respond more often and more favorably to these customized advertising messages. While Yahoo! has not publicly disclosed the portion of our revenue related to interest-based advertising, it is a fast-growing part of our business. To lend context to the revenue opportunity in this area, please consider the following:

A June 2008 eMarketer study indicates behaviorally targeted online advertising was a $525 million market in 2007 but will grow to $4.4 billion by 2012. That represents an expected annual growth rate of over 50%. eMarketer further projects behaviorally targeted online advertising will represent nearly 25% of all U.S. display ad spending in 2012, up from 2.5% in 2007. We believe these growth expectations stem from the fact that users clearly find BT ads more compelling and useful – as evidenced by users clicking on these ads much more frequently. Recent research was published indicating increased click-through rates of up to 670% on behaviorally targeted ads. http://www2009.eprints.org/27/1/p261.pdf. A reduction in the data available to power interest-based advertising systems could reduce our ability to capitalize on this segment of the advertising business that users clearly find more engaging.

This is also true for the many publisher sites where Yahoo! serves advertising because it would create unnecessary barriers to data flows. If such a regime were to emerge, it is unclear that Yahoo! or our industry counterparts would be able to maintain an ad network model, which provides publishers (many of them small or niche players) with the ability to monetize their websites by outsourcing ad sales and serving. Advertising is the only source of revenue for many of the websites that make up the long-tail of the web. These small publishing sites benefit from being part of an ad network that aggregates audiences and provide sophisticated advertising infrastructure across many sites. Many of these publishers do not have the scale to effectively sell or serve advertising on their own, nor would they have the higher user responses that result from customized advertising. Thus, an opt-in

model would significantly reduce the revenue publishers derive from their sites, leading to a reduction in the economic viability of many smaller websites.

Our approach to privacy, as stated in my testimony is based on a front-end/back-end philosophy – a good opt-out coupled with data retention policies that minimize the maintenance of personally identifiable information for long periods of time. As this is clearly a growth area of consumer and advertiser interest, Yahoo! has taken steps to ensure our users have more control over the use of their data for these purposes. We believe that allowing users to opt out of the use of data for interest-based advertising gives users choice while maintaining access to the Yahoo!'s vast array of customized content and services. Yahoo! believes a good opt-out needs to be prominent, readily accessible, clearly conveyed and persistent. We have been a leader in developing appropriate opt-out practices, and we are committed to the spread of similar policies throughout the industry. For those concerned that an opt-out should be of collection versus use, it is important to note not only the important reasons the data is needed listed above in response to questions 3.a., but also that Yahoo! has emphasized the responsible back-end approach described in response to questions 3.b. and 3.d.

4. **What percentage of Yahoo! users know what information Yahoo! collects about them and how that information is used?**

Users of online services are becoming more sophisticated. Yahoo! has received feedback that in some cases our users assume we are collecting and using much more information than we are in fact. While it is impossible to tell how many users actually "know" these positions, it is easy for users to obtain the information in a user-friendly format should they be interested. All Yahoo! users have 24x7, readily available access to information about what Yahoo! collects and how it is used through its privacy policy, which is available on nearly every page of our network. http://privacy.yahoo.com.

Yahoo! is also experimenting with additional ways to surface this information and to provide user controls from places other than the privacy policy, such as in or around an advertisement as mentioned in the response to question 1.

5. **We often hear about privacy settings on browsers. Do changes to those settings impact Yahoo!'s ability to engage in behavioral advertising or interest-based advertising? If so, how?**

Browser settings related to cookies have been around for many years. Browsers can be set to restrict which cookies can be set on a user's computer, or can eliminate the ability to set cookies altogether. Since ad networks are cookie-based, these browser settings have had the potential to affect the ad network business model during this period. In addition, new browser features such as the blocking feature of Microsoft's "in private" mode can restrict information sent in ad calls. When this happens, the advertisement may not show up correctly on a publisher's website or there may not be enough information to serve a customized advertisement. The

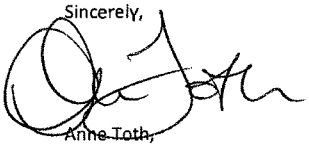
publisher may experience a reduction in advertising revenue in this case because an ad is not shown nor can a user click on an advertisement.

6. **Is there a difference between behavioral advertising and interest-based advertising? If so, what?**

   Yahoo! uses the term "interest-based advertising" as the most appropriate description of our intent to customize ads to users based on their interests. Behavioral advertising has been defined by the Federal Trade Commission in its self regulatory principles as "the practice of tracking an individual's online activities in order to deliver advertising tailored to the individual's interests". Behavioral advertising and interest-based advertising are terms that could be used interchangeably.

Again, thank you for the opportunity to provide you and the Committee with further information about Yahoo! practices.

Sincerely,



Anne Toth,
Vice President of Policy & Head of Privacy
Yahoo! Inc.

YAHOO!

July 28, 2009

The Honorable Steve Buyer
House Committee on Energy and Commerce
2125 Rayburn House Office Building
Washington, DC 20515-6115

Dear Representative Buyer,

Thank you for the opportunity to follow up with additional information responding to questions you have posed in connection with the June 18, 2009 hearing entitled "Behavioral Advertising: Industry Practices and Consumer Expectations". Given the work Yahoo! has done in this area, we welcome the opportunity to provide a more complete picture to the committee for the record.

1. **How realistic is "self regulation" in the industry and is self regulation the best method to protect consumers at this early stage of the market? What can be done to reassure this committee regarding the benefits of self regulation within your industry?**

   Most consumers are becoming increasingly sophisticated about what they want in an online environment, and companies providing services understand that they must provide services in ways that maintain users trust. In fact most, if not all, advances in online privacy protection have come as a result of industry self-regulation. that builds this trust. Competition encourages companies like Yahoo! to make privacy tools available to our customers as quickly as we can develop them. As one company leads, many others follow or leapfrog by innovating in other ways. This competition has led to innovations in user notice, choice, security, and enforcement. One of the reasons these self-regulatory initiatives have been successful over the last decade is that companies like ours responded quickly as markets evolved and services became more and more sophisticated.

   The pace of change online has also been a driving factor in our self-regulatory efforts. Since the Internet became commercial in 1995, online companies have developed best practices in areas such as child protection, security, and privacy practices, responding to consumers' need to feel confident in this new medium. Just as new services evolve so too do best practices. For instance, in the early days of the Internet, many services gave no indication of what data they collected or used when a user visited a website. It is now standard practice to include a link to a privacy policy on the home page of Internet websites. These policies include statements about the collection and use of personally identifiable information, and serve to educate consumers about the choices they have. Furthermore, the FTC and individuals can hold the website responsible in courts of law for the representations made in its privacy policy.

   In addition to self-regulating, Yahoo! has also played a role in larger industry-led consortiums. As the need to address Internet consumer issues has grown, several trade associations and third party enforcement groups such as the Network Advertising Initiative, the Interactive Advertising Bureau, the Online Publishers Alliance, the Direct Marketing Association, TRUSTe and others

have played an increasingly important role in self-regulation. These organizations may focus on one or just a few aspects of the larger online ecosystem, but they each play an important role in moving the industry toward more responsible practices and standardization of those practices.

Perhaps the latest example of self-regulatory initiative is the set of principles recently released by the American Association of Advertising Agencies (4A's), the Association of National Advertisers (ANA), the Direct Marketing Association (DMA), and the Interactive Advertising Bureau (IAB), among others. From the press release found at http://www.iab.net/about_the_iab/recent_press_releases/press_release_archive/press_release/pr-070209, "The Council of Better Business Bureaus (BBB), a leading organization dedicated to advancing marketplace trust, is also part of the effort and has agreed, along with the DMA, to implement accountability programs to promote widespread adoption of the seven Principles. This cross-industry self-regulatory task force represents the first time that representatives of the entire advertising ecosystem have come together to develop principles for the use and collection of data in this important area to the economy." Yahoo! is pleased many players in the online advertising ecosystem previously not engaged are making public commitments. We are working with these organizations to bring these principles to the implementation stage including additional tools for users.

In addition, last year many search engines announced new policies concerning the retention of search data – and in Yahoo!'s case – all web log data. For some of these companies, this marked the first time they had publicly stated policies around retention, anonymization or deidentification of search data. After one company announced they would retain data for 18 months, others announced policies of 13 months and 18 months but with differing anonymization techniques. At the end of 2008, Yahoo! announced a new data retention policy committing to anonymize server log data - including page views, page clicks, ad views, ad clicks, and searches - after 90 days. Server log data that is routed to systems Yahoo! uses to help prevent fraud and preserve security will be retained for up to six months – but only for that purpose. Yahoo! also must retain data longer in some instances to comply with legal obligations. This move to cover server logs is a significant expansion from our original policy that applied only to search log data at 13 months, and is being implemented on a global basis by mid 2010. This is a strong indication that industry is responding to consumer demand and competitive pressures with respect to data policies, and should thus reassure the committee that much can and is being done in the marketplace to self-regulate.

2. **Do you believe Congress should pass a bill regulating entities or the conduct of entities? Furthermore, do you believe the FTC or the FCC is better equipped to handle the regulation of these entities and their conduct regarding Behavioral Advertising?**

The online industry has worked for over a decade in partnership with the Federal Trade Commission to strike the right balance between self-regulation and government oversight. The FTC has developed significant expertise in this area and, as such, we believe that online privacy should primarily be under the purview of the FTC rather than the FCC. There are historical reasons why some entities - primarily network operators - have had their collection and use of data regulated by the FCC and we think that Congress should tread carefully to ensure that

there is both consistency in regulation and protection of consumer information as technologies and services converge.

In addition, we do believe that two entities doing the same thing with the same technologies should be regulated in the same way. However, there are many business models proposed in the online advertising space and each should be examined individually. For instance, an entity with access to all Internet web browsing behavior as a condition of receiving service is vastly different from a model where cookies may be set on a user's machine over time. In the latter example, all user activity is not logged and users have meaningful and easy-to-access controls to delete the cookies. These and other differences should not be ignored when policymakers consider how to treat various business models.

3. **Do you favor an across-the-board approach to regulation with equitable penalties and enforcements? If so, does that mean you support a single regulatory agency to oversee Behavioral Advertising?**

As mentioned above, Yahoo! favors self-regulation in general. We believe that any regulation – be it government or self-regulation – should adopt a front-end/back-end approach that will be most effective for all players in the online advertising space. However, there are many factors that come into play with respect to data collection and use for interest-based advertising. Two entities doing the same thing with the same technologies should be regulated in the same way. Where differences exist in the type of data collected and used, the sensitivity of the data (e.g., is it personally identifiable?), the ability for users to control use of the data, the transparency around data practices, or how the data is secured or stored, there should be recognition of the differences and how they are treated under any regulatory regime. Penalties should be commensurate with the severity of an offense. Yahoo! believes the agency with clear authority over online advertising practices is the FTC. The agency has been driving industry to innovate and self-regulate responsibly with tangible results.

4. **Are there any benefits to having both the FTC and FCC involved as regulatory entities?**

With respect to online advertising, the FTC has developed significant expertise, so Yahoo! believes that online privacy should primarily be under the purview of the FTC rather than the FCC. There are historical reasons why some entities — primarily network operators — have had their collection and use of data regulated by the FCC and we think that Congress should tread carefully to ensure that there is both consistency in regulation and protection of consumer information as technologies and services converge.

5. **What is your view of an approach that some have recommended which would in effect be modeled after the "do not call list" and would be a "do not track list"? Should consumers be provided this opportunity?**

Consumers should be afforded the opportunity to control the use of their data for interest-based advertising purposes. This can be done in a number of ways – either via websites visited,

a central website representing numerous online ad delivery networks at once such as the NAI website www.networkadvertising.org, or through browser tools that eliminate cookies or allow "in private blocking" mechanisms. Many companies and websites are building browser plug-ins and other tools to offer persistent opt-out cookies so that a user's choice is respected even if cookies are deleted.

Some of these options have the effects similar to a "do not call" or "do not track" list, but are different in important ways. In the "do not call" world, users have consistent phone numbers issued by one provider. However, in the online space, IP addresses are often dynamic even when set by one provider. Online advertising is largely customized based on the use of cookies, which are set by thousands of entities and undergo enormous churn (meaning users delete their cookies or cookies are reset). These fundamental disparities make the idea of a "do not track" list challenging to say the least.

6. **According to the FTC Staff Report of February 2009 on this behavioral advertising issue: "Many of the companies engaged in behavioral advertising are so-called 'network advertiser' companies that select and deliver advertisements across the Internet..."**

   a. **Who are these network advertisers?**

      Network advertisers are entities that partner with hundreds of websites (often small or niche website publishers) in order to create economies of scale so that advertisers are willing to purchase advertising. The network advertiser is able to work directly with advertisers on behalf of the publishers in its network of sites so that the individual publishers do not have to individually negotiate ad deals with each advertiser. One example might be a site focused on German Shepherds, which joins an ad network in order to find advertising for its 80,000 users. An advertiser may not be interested in such a small audience, but when paired with other sites in the ad network, the advertiser can market to the larger audience it is looking for. In this way, network advertisers serve an important function bringing together buyers and sellers of advertising, which in turn provides the revenue the publishers of the websites need in order to pay for internet connections, web hosting, content and services they provide to users – usually for free. The NAI offers more information and a list of members at http://www.networkadvertising.org/participating/.

   b. **Can you give me a few examples of which companies that you believe that the FTC staff must have had in mind when it made this reference to network advertiser companies?**

      Yahoo! believes it is likely the FTC was referring to the NAI member companies. http://www.networkadvertising.org/participating/.

   c. **Are we, in the main, talking about companies such as Google, Microsoft and Yahoo!?**

      NAI members have grown significantly in the last 18 months and now includes over 30 member companies. Membership has doubled in the last year alone. Google, Microsoft

and Yahoo! joined the NAI after purchasing companies with ad network business models. While there are no official measures to point to, Yahoo! believes that the majority of interest-based ads served on the Internet are served by NAI member companies.

7. **Behavioral advertising is targeted to a specific individual based on that individual's web surfing behavior. Which entities are the predominant users of this type of advertising?**

First, it is important to clarify that often-times interest-based advertising is not targeting a specific individual but the user of a particular IP address or computer. This distinction is necessary because much interest-based advertising is done without any connection to a user's real identity.

Second, it is not that some companies are users of this method and some are not – a better way to think about the marketplace is as an evolution to more efficiency in the advertising market. In today's economy, where companies have limited resources to spend on advertising, they want their advertising dollars spent in the best possible way. Advertisers are looking for ways to reach their customers more directly, rather than wasting money placing ads in areas where they will have no impact. Behavioral advertising has grown because it has been shown to be quite effective – measured by the frequency of user clicks to learn more about such ads – in reaching particular users.

Recent research was published indicating increased click-through rates of up to 670% on behaviorally targeted ads. http://www2009.eprints.org/27/1/p261.pdf. A June 2008 eMarketer study indicates behaviorally targeted online advertising was a $525 million market in 2007 and would grow to $4.4 billion by 2012. eMarketer further projects behaviorally targeted online advertising will represent nearly 25% of all U.S. display ad spending in 2012, up from 2.5% in 2007. It is because users clearly find them more compelling and useful that more and more advertisers purchase this form of targeting.

8. **Some have questioned the Network Advertising Initiative (NAI) effectiveness due to the manner in which it has been set up and so few members. Is it a model that is the best we can offer or to truly make a difference should be a larger, more diverse body?**

Yahoo! became an NAI member after beginning to serve advertising on sites other than Yahoo.com in 2007. We joined because of the work NAI had done to date to establish baseline practices for entities serving ads as third parties. The NAI was quite small at the time, but has since grown dramatically from 15 members to 29 members in the past year, with more membership applications pending. The ten largest advertising networks are each members of the NAI. The NAI also expanded beyond its roots with advertising networks to include leading data exchange and marketing analytics service providers. As it was growing and the industry was evolving, the NAI embarked upon a significant update to its existing self-regulatory practices. The new practices can be found at http://www.networkadvertising.org/networks/principles_comments.asp. It is clear the NAI has been responding to the changes in the marketplace.

Even so, the NAI does not represent the entire online advertising ecosystem. That is why the recent announcement of the IAB, AAAA, ANA, DMA and others embracing self-regulatory principles was also a welcome effort. These new principles, when implemented, will give users easier access to information they need and controls they may want with respect to online advertising practices. This group represents a much larger group of online players including advertisers and their agencies, website publishers, and a broader set of marketers. Yahoo! works with each of these groups as we work toward responsible policies for all sectors of the online advertising ecosystem.

9. What benefits does "Behavioral Advertising" have for the electronic ecosystem?

The advertising model has made Internet content and services available to millions of people in the United States and around the world – for free. The business model of relying on advertising revenue to fund websites has meant that vast amounts of information on the Internet has been fully accessible to people of all ages and income levels. The trend over the past few years, exemplified by steps by AOL, the New York Times and the Wall Street Journal websites, has been to tear down economic barriers to content – possible only because the primary source of revenue for most content providers' online operations is an advertising, rather than a subscription, model.

The benefits do not end with a rich diversity of content. Consumers also experience enhancements as they receive customized content, services and advertising that save them time and money. For instance, many have become used to websites storing our information while giving us easy "one-click" access from anywhere an Internet connection can be established. Many users frequently use recommendations for new products and services they trust – some from advertising sources. And the exponential growth of social networking sites demonstrates a clear interest in customizing the online experience. Everyday information such as weather, local news, mail alerts, stock alerts, and offers for products or services users are interested in is provided through customization techniques. Most of these technologies have been the result of investments by companies funded by their online advertising revenues.

Advertising directly supports the creation of Yahoo!'s industry leading services. Yahoo! maintains industry leading sites including finance, sports, news, personalized home page, mail, shopping, travel and more. Many of these products are multi-award winners and are updated with new features and functions regularly. Other services to our users such as anti-spyware software, unlimited mail storage and generous photo and video storage are also provided for free because of the advertising model.

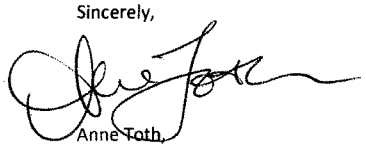
Advertising also supports a diversity of voices on the Internet. Bloggers or families who want to occasionally post content are generally subsidized by the advertising business model through free or reduced-cost hosting, and also through the ability to have text, graphical and even video ads appear on the site. This ability to make money while sharing views increases the number of viewpoints that can be taken in public debates, and surely enriches our public conversation as a nation and as a global society.

Yet another benefit is the rise of small businesses that have been able to gain a foothold on the Internet with very low barriers to entry. These small businesses are able to make a profit in part because new tools are available to carry advertising on their sites, giving them another source of revenue. And the type of advertising is relevant here. These small businesses can sell advertising on a wider range of topics when the advertising can be tailored to user interests, even if the site is primarily about a different topic.

Given the wide range of benefits to society to consumers, bloggers, small businesses, and even advertisers who can more efficiently find the right audience for their messages and offers, it is important to give due weight to these benefits when exploring the appropriate framework for discussions of online advertising issues.

Again, thank you for the opportunity to provide you and the Committee with further information about Yahoo! practices.

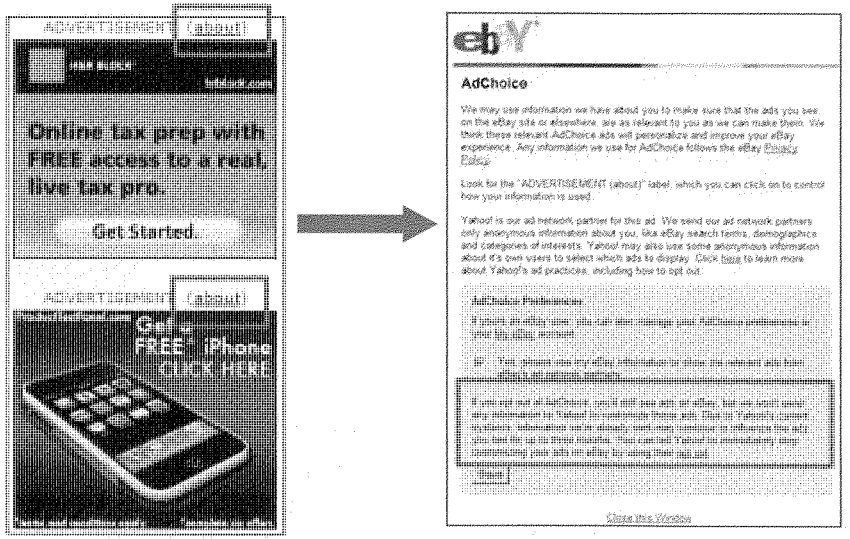
Sincerely,



Anne Toth,
Vice President of Policy & Head of Privacy
Yahoo! Inc.

Attachment A
eBay AdChoice Program

Attachment A
Contextual Ad Notice: EBay AdChoice



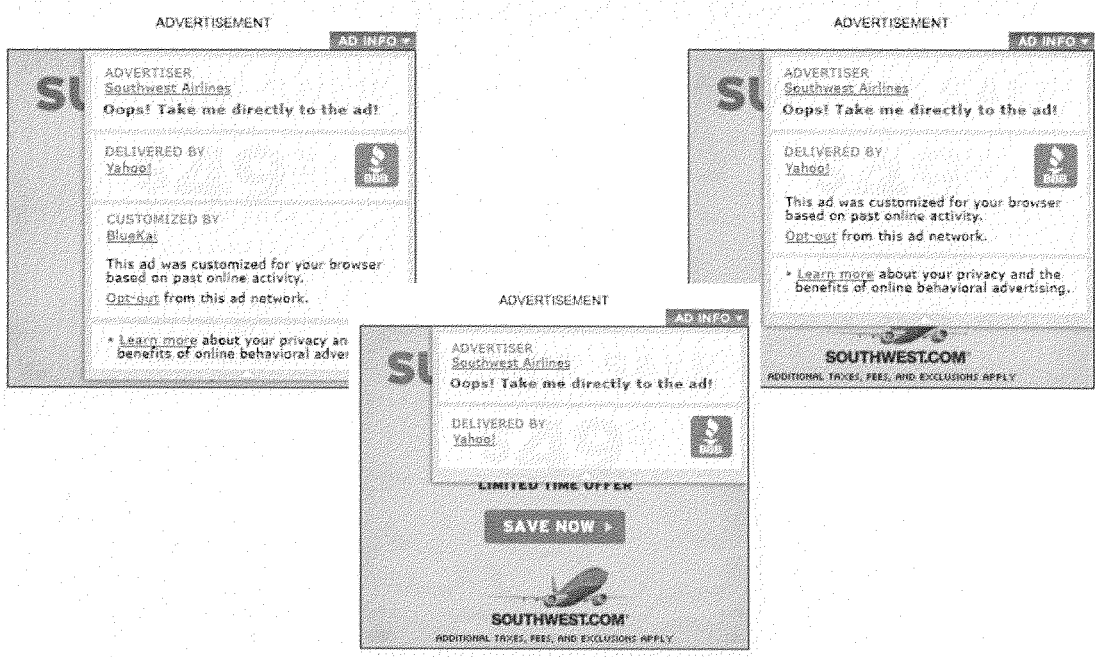
Attachment B
CLEAR Ad Notice
Control Links for Education
and Advertising Responsibly

CLEAR Ad Notice (CAN) Technical Standard

Version	CAN-ver()	Provides the version of the CAN Standard being used so publishers and tools can appropriately process the passed information.
Ad Link	CAN-ad()	Provides the link of the ad to present to the user in case they have clicked on the Ad Marker in error and can proceed to the ad destination without needed to close the Interstitial.
Advertiser Name	CAN-adn()	Provides the legal business name of the advertiser responsible for developing and placing the advertisement
Advertiser Link	CAN-adl()	Suggested this links to the advertiser's home page or page explaining their advertising practices and partners
Network Name	CAN-ann()	Provides the legal business name of the ad network responsible for the placement of the advertisement
Network Link	CAN-anl()	Suggested this links to the network's advertising practices and control (opt-out) page
Matcher Name	CAN-man()	Provides the legal business name of the party providing matching services for the ad
Matcher Opt-Out Link	CAN-mol()	Suggested this links to the matching party's interest management or opt-out page
Matcher Manage Link	CAN-mml()	Suggested this be used in situation where a party host separate interest management and opt-out links
Match Flag	CAN-maf()	Is behavioral targeting used for this ad – Y/N?

Possible Examples of Label

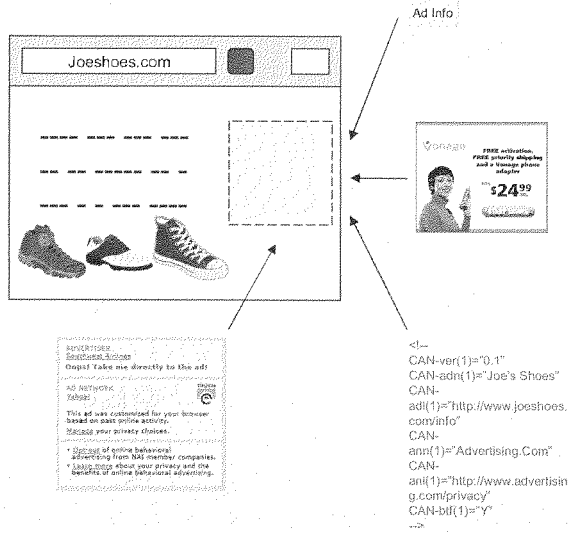
Interstitial Examples



Multiple Approaches Possible

- Publisher Manages Notice
  - CLEAR Ad Notice: Publisher develops Ad Slug or Overlay script and inserts the script where each ad call is made
  - CLEAR Info Tag: Ad server passes data with each ad served
  - CLEAR Interstitial: Publisher develops Interstitial script and adds it to each page where ads are served (activated when CLEAR Ad Notice is clicked on)
- Ad Network Manages Notice
  - CLEAR Ad Notice: Ad Network develops Ad Slug or Overlay script and serves the script with each ad
  - CLEAR Info Tag: Ad Network passes data with each ad served
  - CLEAR Interstitial: Ad Network develops Interstitial script or web page and serves this with each ad as well (activated when CLEAR Ad Notice is clicked on)

CLEAR Components



Component	Served By	Options
Ad Marker (Slug) or Ad Overlay	Either Publisher or Ad Network	Can place adjacent to ad (Ad Slug) or on top of ad (Overlay)
Ad	Ad Network	As done today
Info Tag	Ad Network	Can support multiple versions / metadata types
Interstitial	Either Publisher or Ad Network	Can be served as "overlay" script or as a separate page

Attachment C

Yahoo! Data Retention Policy & Process

Data Retention Policy

Enhanced Global Data Retention Policy

- Industry leading both in dramatically shortening retention duration and significantly broadening scope of data covered under the policy

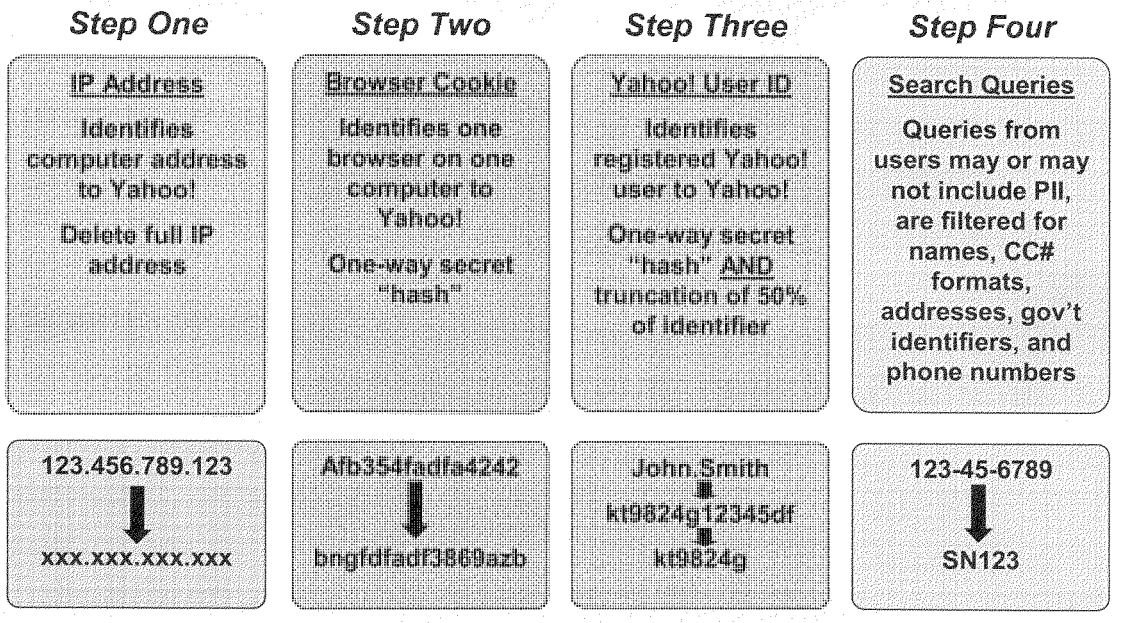
Duration

- Up to 90 days for most log file data
  - Many systems will retain for less than this period
- 6 months for select log file systems:
  - Product fraud detection – click fraud example
  - Abuse management
  - Financial fraud tools
- Access controls employed
- Exceptions for specific legal obligations

Scope of Data

- Search log files… AND
- Page views
- Page clicks
- Ad views
- Ad clicks
- Policy now applies to log files that serve all products and ad platforms, not just search

Anonymization Process for Identifiers - 4-Step Process



This document was created with Win2PDF available at http://www.win2pdf.com.
The unregistered version of Win2PDF is for evaluation or non-commercial use only.
This page will not be added after purchasing Win2PDF.

Responses from Chris Kelly
Chief Privacy Officer
Facebook, Inc.
Questions Propounded by Ranking Member Radanovich (R-CA)
Dated July 14, 2009
Hearing Regarding Behavioral Advertising: Industry Practices and Consumer Expectations

1. Who owns the information, pictures, etc., once uploaded by a user to your website?

Users of our service retain ownership of information they upload to our site, and our privacy settings give them control over who has access to that information.

2. How can a consumer erase their information from your website? What is the justification that a user must delete each piece of information they uploaded before deleting their account in order to ensure their privacy is protected rather than lingering on a backup tape somewhere?

Facebook offers users a number of different options to make their data they have uploaded to our service unavailable. These options reflect user preferences based on our experience. Most choose to deactivate their accounts for temporary reasons, which does render their account invisible to users of the Facebook service. Their friend connections, pictures, videos, and other content are then available to them upon their return.

We also offer a deletion option that entails a fuller scrub of personal information from Facebook's databases. Those users who pursue this option have critical account information purged and are thus unable to recover their content and friend connections if they return to the service. This option takes effect roughly 14 days after it is requested.

The reference in the question to the "delet[ion] of each piece of information [the consumer] uploaded" is based on a policy that changed more than two years ago with the introduction of the blanket delete option.

3. Facebook's privacy policy states it "may also collect information about [users] from other sources, such as newspapers, blogs, instant messaging services, and other users of the Facebook service." If that is the case, is a user really in control of what Facebook can collect and use?

The language quoted in the question does not include the sentence that follows – "Where such information is used, we generally allow you to specify in your privacy

settings that you do not want this to be done or to take other actions that limit the connection of this information to your profile (e.g., removing photo tag links)."

Facebook strives to give users control over collection and use of information and its introduction of robust and specific privacy tools has led to more sharing and control throughout the Internet.

4. Your written testimony references Facebook Connect, a new feature of Facebook.com for interaction with other webistes. Is this information sharing program opt-in or opt-out by default?

Use of Facebook Connect is on an opt-in basis. Users choose whether to connect their account with the third party websites where Facebook Connect is an option.

5. Your written testimony emphasized that control over and access to personal information is a core Facebook principle. The Facebook privacy policy states that it permits third party advertisers to place cookies on users' computers and that these cookies may track and compile information. Further, the privacy policy emphasizes that Facebook's privacy practices are not binding on these third parties. If installation of these cookies is facilitated by the user of Facebook, are Facebook users then able to prevent such installation by some function on the Facebook website?

Browsers such as Firefox, Internet Explorer, and Opera offer extensive controls to block all third party cookies for any users who are so inclined.

6. Your written testimony stated Facebook uses non-identifiable information to drive ads to users while on its website. Whether or not a user's name is included with this information, and whether this information is retained or transmitted, this may still be personal information that some people may not be comfortable being tracked or used. Why shouldn't consumers be able to opt-out of such use of their information?

Consumers who have particular sensitivities in this area are of course welcome to refrain from the use of Facebook's free service, but the aggregated use of data for the targeting of advertising in a real-time basis seems to be a fair tradeoff to assure that a good user experience is delivered and Facebook is able to continue to deliver the service for free.

7. Facebook has in the past used users' likenesses, without their knowledge, in commercial advertisements to other users to say, "so and so is a fan of this widget, click here to buy."
    a. Is this still a Facebook practice?

Facebook's innovative Social Ads are presented with the full knowledge of users – they are regularly shown in the spaces reserved for advertising, giving users real-time notice about the possibility. Furthermore, users are able in their privacy settings to block the use of their name or image in Social Ads for their friends. Social Ads are not presented to non-friends. The basic operation of Social Ads is no different from the promotion of actions in the stream that forms each user's basic homepage on Facebook – the same content (e.g., whether a particular user has become a fan of a particular page) is presented.

    b. If so, should a consumer not have the choice as to whether or not their likeness is used in a commercial advertisement driven to another user?

Consumers do have a variety of choices with regard to their participation in Social Ads through Facebook. First and foremost, they have a complete opt-out setting that is readily available from our Privacy page. They are also free to restrict the display of actions they take through their privacy settings, settings that are respected by the Social Ads system. Finally, they are of course able to refrain from taking actions on Facebook.

8. Although the industry continually tries to improve privacy policy notices to make them more user-friendly, such notices remain long and complicated legal documents. Is there utility in trying to create a "nutrition label" type approach – a uniform and easily recognized notice – so consumers can "comparison shop"?

Facebook has for more than three years had a "layered" privacy policy, where we provide a basic statement of our principles at the beginning, and then get into more particular descriptions of our practices in the fuller policy. We are dedicated to comprehensive user understanding and a plain language approach to all our documents, shown most recently in our adoption of a Statement of Rights and Responsibilities to replace our old Terms of Use. The Statement of Rights and Responsibilities was ratified by users in an innovative notice, comment, and voting procedure that received worldwide notice and that we believe will serve as a model for Internet companies in the coming years. The privacy policy will go through a similar procedure when it is revised and updated in the near future.

While the idea of a uniform form of notice is attractive on the surface, the problem with pursuing uniform notice across many sites is that many services are innovative and describing them using old categories will inevitably leave users with misimpressions as to the actual usage of their data. We are strong advocates of

giving users direct choice and control about what information is shared with whom through robust and specific privacy controls. In fact, Facebook is an industry-leading privacy innovator and expects to continuously update its privacy settings and policies to further empower our users with respect to their data. Consequently, a uniform notice template shortly might become outdated and not representative of the unique, advanced tools that Facebook provides our users.

28 July 2009

Honorable Henry Waxman
Chairman
House Commerce Committee

Honorable Cliff Stearns
Ranking Member
Subcommittee on Communications, Technology, and the Internet

Dear Congressmen Waxman and Stearns:

I am happy to answer the questions sent to me on July 14, 2009.

1. As someone who has spent considerable time examining the behavioral advertising field, whether for my book [*Digital Destiny: New Media and the Future of Democracy*, 2007], a series of regulatory filings at the Federal Trade Commission [submitted with U.S. PIRG), a number of professional articles and reports [such as the forthcoming "Interactive Food and Beverage Marketing: Targeting Adolescents in the Digital Age, *Journal of Adolescent Health*, September 2009], and websites addressing the issue [such as my digitalads.org], I believe that consumers do not have any substantive understanding of the different technologies used for behavioral advertising. My written testimony for the June 2009 hearing explored in some detail the range of elements that comprise, as advertisers call it, the "high definition media and marketing ecosystem." Consumers generally have no idea about the various behavioral targeting technologies and strategies, including ad exchanges, retargeting, predictive behavioral targeting, the use of outside databases, etc. Nor are they aware of the relationship between search and display digital advertising, the role of so-called "immersive" rich media designed often to aid in targeting and data collection, or data collection performed in online games and in virtual worlds, etc. I agree that regardless of the techniques and strategies used both to foster the collection of information and to use it for profiling and targeting, consumers should first be informed—and have the right to control—all data collection that is used for profiling and targeting.

2. A consumer-centric approach, as suggested by your letter, is the best approach. It should be technologically neutral and apply to everyone in the online advertising market. But additional safeguards are required for network operators using so-called deep packet inspection or other

technologies available to Internet Service Providers. While giant search and online ad companies, such as Google, Yahoo, Microsoft, and Time Warner's Platform A, collect a tremendous amount of data on consumers, as do online advertising networks, they still do not have the ability to engage in the kind of 24/7 monitoring that ISPs will be able to undertake (especially the handful of cable and telephone companies that dominate the U.S. broadband access market). As you know, ISPs have actual financial records on individual consumers, which can be integrated into their profiles based on an analysis of their online behaviors (which can also be expanded to include their TV viewing and mobile phone characteristics). ISPs engaging in behavioral profiling and targeting should be required to provide consumers with greater safeguards. I personally believe it would be preferable if ISPs were not permitted to engage in behavioral targeting. Any form of "one-stop shopping" data collection should be avoided. Such revealing records could be accessed by government and others and pose new threats to the civil liberties of Americans.

3. I agree that consumers should be in complete control over the data that is collected about them. That's why an affirmative opt-in after full and meaningful disclosure are necessary. Companies should be required to completely inform consumers about what data will be collected and how it will be used. This should include explaining to consumers how information might be added to their profile, such as data based on subsequent tracking or via amplification from outside databases. But sensitive information—especially financial, health, medical, and family-related (and data connected to children and adolescents in particular)—require additional consumer safeguards. Nor should data on consumers be kept for more than 90 days; it should then be destroyed. Consumers should have the right to renew their opt-in agreements every 90 days. But beyond consumer control, Congress must further explore the data collection system that has been created for the online environment, including for mobile marketing. There should be limits placed on what industry can do with certain data collection practices.

4. There should be uniform standards protecting consumers across the digital marketing/targeting industry. In a market where the baseline is the collection of data on individual consumers for a range of micro-targeting practices using very powerful and sophisticated (and largely stealth) techniques across all platforms, which is designed to influence behaviors and attitudes, Congress must ensure there are meaningful safeguards. Beyond these standards, companies will offer consumers competing and alternative approaches related to privacy protection.

5. A consumer-centric model should foremost protect our most sensitive information, including health and financial data. As the Committee is well

aware, our society is rapidly moving to a system where more of our critical transactions will be conducted online (either in part or entirely). From mobile banking, to searching for mortgages online, to queries about life insurance or searches about health concerns, the online environment will be the medium of choice for many of us. Information collected from both children and adolescents also fall into a category defined as sensitive. I also believe that a person's ethnic or racial background should also be deemed sensitive data. Congress should enact online privacy legislation that specifically identifies what is considered sensitive data. This should include all data involving financial, health, racial, and children/youth categories.

6. Consumers do not have the tools to exercise meaningful consent with regard to online advertising. As we told this Committee, companies should be required to inform consumers about the full range of data collection and usage practices prior to any collection for profiling and targeting. The current system has been constructed to be deliberately opaque, because many online advertising companies know that if consumers were truly informed of the practices employed, they would likely not consent to such data targeting. Companies should be required to develop a "plain vanilla" online disclosure prior to any data targeting. Prominently placed on home pages and linked to easy to understand descriptions, consumers would be informed of what data is collected, and how it is used. We are convinced there are effective ways to balance both the consumer protection and privacy interests of users with the need to ensure the continued robust growth of electronic commerce.

7. I believe that data collection from first-party websites is also a serious privacy concern. The question is correct in its assumption that a first-party advertiser, including those with affiliated interests, can collect significant amounts of data from consumers. Privacy rules are required governing both first- and so-called third-party sites and services.

8. Online marketers will financially benefit from a government-backed privacy regime. Consumers will have greater trust in the process, and more dollars will flow to online services. Privacy will not cause the Internet to file for bankruptcy, as some online marketers have suggested. The current crisis should be a telling reminder to all of us what can happen when there isn't reasonable and responsible regulation. As consumers further rely on the Internet for all manner of transactions, they need to be assured that their interests are protected. This will provide for consumer confidence that will actually help online marketers prosper.

9. Consumer information, especially concerning individuals, is a very valuable commodity. Data is being collected about consumers without getting their informed consent, nor with any real understanding of how it's being used.

While online advertising helps support a broad range of free services online, the price consumers are paying via the unfettered use of their information raises serious concerns about unfairness.

10. An explicit consent regime would require the companies to honestly inform consumers. Consumers would, in our opinion, likely agree to a range of data collection practices if they understood and controlled the process. Companies should be required to obtain explicit consent and then compete in the marketplace.

11. There is a range of interactive marketing techniques and not all require the development of a more detailed profile. For example, companies that understand the online buying cycle for a particular product (say an auto) and have the ability to track a profile and then "retarget" a user at the right time (using perhaps editorial assets that have been identified as of interest to the consumer), can be potentially as effective as a company that has amassed a more complete dataset on a user. But I do believe that companies that have more complete information of a user (depending on that person's demographic characteristics and whether they are considered valuable to a advertiser) will be able to charge more.

12. First- and third-party advertisers should be treated the same way. Google is both a first and third party advertiser, given its extensive data collection assets.

I am happy to provide additional information, including citations.

Sincerely,

Jeffrey A. Chester
Executive Director
Center for Digital Democracy
Washington, DC
www.democraticmedia.org

NAI
Network Advertising Initiative

July 28, 2009

Hon. George Radanovich
Ranking Member
Subcommittee on Commerce, Trade, and Consumer Protection
Committee on Energy and Commerce
2125 Rayburn House Office Building
Washington, DC 20515

Dear Ranking Member Radanovich:

Below please find the responses from the Network Advertising Initiative to your written questions in connection with the June 18th joint hearing entitled "Behavioral Advertising: Industry Practices and Consumers' Expectations."

1. **Is the best privacy policy a consumer-focused policy? Should Congress require more rigorous consent when a company uses information in a way that is not directly related to the primary purpose for which the consumer provided it? For example, when a consumer goes to a web site to stream video, consent to collect information such as the consumer's IP address and web browser type may be assumed because this information is necessary to deliver the video stream the consumer requested. However, more explicit permission would be necessary to use that information for unrelated purposes. What are your thoughts on this type of approach?**

The member companies of the Network Advertising Initiative (NAI) help operators of Web sites and services (Web "publishers") to deliver interactive display advertisements. NAI members use Web browser cookies to serve these Web publishers' visitors with more relevant and compelling consumer advertisements. The revenue from such advertisements allows Web publishers to continue to offer the vast majority of their services free and without charge to consumers. The advertising networks, exchanges, and other business models represented in the NAI are integrally involved in the operations of Web publishers, both large and small. They help publishers find advertisers for their audiences; enhance the relevance of the advertisements served to their users; and measure the effectiveness of these campaigns for advertisers.

Consequently, advertising-related services are not "unrelated" to the operations of ad-supported Web publishers – they are directly related to the ongoing success of their business model, insofar as these publishers derive revenue from the collection and use of advertising-related data by other companies, including NAI members. In today's Internet ecosystem, consumers have strongly demonstrated a preference for such ad-supported, free-of-charge Web content and services, rather than a paid subscription approach.

Any adoption of an "explicit permission" requirement for the collection and use of advertising-related data could profoundly alter the consumer experience for Web-based services. Consumers could face a barrage of "explicit permission" prompts for advertising data collection. More importantly, such an "explicit permission" approach could adversely affect the fundamental revenue model supporting the ad-supported services that tens of millions of consumers enjoy today (such as news, blogs, video, photo-sharing, and social networking services.)

The NAI believes that its self-regulatory model for online behavioral advertising strikes the right balance in consumer expectations for today's cookie-based advertising services: the model combines an opt out for the use of non-sensitive, non-personally identifiable information to deliver ads, with an opt-in requirement for uses of certain sensitive or personally identifiable data.[1] The NAI's self-regulatory Code mandates that its members provide clear and conspicuous notice and an opt-out mechanism for online behavioral advertising that involves non-personally identifiable information. However, the NAI Code also requires opt-in consent in two different circumstances: (a) for any uses of sensitive information for online behavioral advertising; and (b) for the merger of personally-identifiable information with data previously collected about users' past Web browsing activity on a non-personally identifiable basis.

Accordingly, under the NAI approach, "explicit permission" – in the form of an opt-in – is not required for all advertising-related activities carried out on Web publisher pages: instead, such permission is instead reserved for circumstances that would be potentially material to the consumer. The NAI believes that such an approach preserves a default experience for consumers in which Web sites provide their users with more, rather than less, relevant advertising, and which at the same time affords them meaningful control of data collection and use for online behavioral advertising and opt-in consent in appropriate circumstances.

2. **Although the industry is continually trying to improve privacy policy notices to make them more user-friendly, such notices remain long and complicated legal documents. Is there utility in trying to create a "nutrition label" type approach—a uniform and easily recognized notice—so consumers can "comparison shop"?**

Privacy policies provide a very significant means for full and complete consumer disclosure, and an accountability mechanism for Web publishers both in for data privacy and security. At the same time, however, consumer disclosure in connection with a variety of privacy-topics can be supplemented by other, shorter forms of consumer

[1] It is important to recognize that cookie and similar browser-related technologies allow advertising services to be provided on a non-personally identifiable basis. When a Web publisher contracts with an advertising network to help serve ads on its Web site, it authorizes the ad network to serve ads from its own servers onto the Web publisher's site. It may also allow the ad network to place its cookies in the browser of visitors to the Web site. Web publishers are not, however, obliged to share information about their user's identity: indeed, for the ad network, the user's actual identity may be entirely unnecessary in order to carry out advertising-related functions. As a result, when information is gathered by an ad network using cookies, the ad network need not combine information about the user's actual identity with user interest or preference information that is associated with the unique identifier in the browser cookie.

notice. There have already been efforts to provide such alternative forms of consumer notice to allow users to more easily "comparison shop": some Web publishers (including many NAI members) already offer "short form," consumer-friendly summaries of key features of their privacy policies; and the P3P standard affords Web publishers the opportunity to present their privacy policies to under a standard taxonomy that is automatically readable by consumers' Web browsers.

For online behavioral advertising, the NAI has long promoted a standard approach to industry disclosure, requiring that its members provide clear and conspicuous notice and choice on Web sites. Through the NAI Web site (www.networkadvertising.org), the NAI also allows consumers to learn more about and opt out of online behavioral advertising by any or all of the NAI's member companies, across the many thousands of Web sites on which such advertising is served.

The NAI also supports recent industry-wide efforts to deliver "enhanced" notice of online behavioral advertising in or around display advertisements. Marketplace adoption of a consistent approach to such "enhanced notice" – whether through the implementation of standardized consumer-facing disclosure language or industry "icon" – would accomplish the goal of allowing consumers to more easily identify online behavioral advertising occurring on the different Web sites that they may visit; and to exercise choice not to receive such advertising or to "comparison shop" for Web sites not allowing such advertising.

3. What information do your member companies collect?

    a. How do your member companies use the information they collect?

    b. How long do your member companies keep the information they collect?

    c. With whom do your member companies share the data they collect?

    d. How do your member companies "anonymize" the data collected and after what period of time do your member companies "anonymize" the information?

    e. How do your member companies ensure they share only the minimum amount of information necessary for their purposes?

    f. What exactly can a user opt-out of?

    g. How would a full opt-in versus a full opt-out regime impact your member companies' businesses?

The data collection and use practices of the NAI members companies vary according to the particular type of online advertising services they provide in the marketplace. At the same time, all NAI members are required to clearly and conspicuously post notice on their Web sites that describes their data collection, transfer, and use practices, either for

online behavioral advertising or other types of advertising-related services. [2]

Although NAI members may collect information on their own Web sites, their primary source of data collection occurs on the partner Web publisher sites on which advertising-related data is gathered. As previously discussed, this generally occurs on a non-personally identifiable basis from Web site visitors, using cookies and similar browser-related technologies. The types of information collected may include information such as a Web site visitor's IP address; date and time; domain type; Web pages that have been viewed by the site visitor; and responses by the Web site visitor to advertisements delivered by the NAI member company or other third party advertising technology vendors. Depending on the Web site partner, the information collected may also include demographic data relating to the user (gender, age, e.g.), geographic data, or other user interest data.

Additional responses to the subsection questions follow below:

(a) The different types of information used by NAI member companies include ad delivery functions (statistical reporting & ad frequency capping, e.g.); ad reporting (advertiser reporting & campaign performance measurement, e.g.); attempted prediction of user interests, characteristics or preferences in order to serve more relevant advertisements (including online behavioral advertising across non-affiliated Web sites); and other related purposes (audience and advertiser research, e .g.).

(b) The NAI Code requires that member companies retain data collected for online behavioral or other advertising purposes be retained only as long as necessary to fulfill a legitimate business need, or as required by law,[3] and also to specify their retention periods. The specific business retention periods for such data vary according to NAI member company and data types: the retention of some interest-related data may be short-lived (user purchase intent data kept only for weeks or months e.g.), while other types of data (demographics or general subject matter interest, e.g.) may be retained longer. Additionally, some companies may retain data for auditing and fraud prevention (click-fraud detection, e.g.).

(c) NAI members that function as B-to-B advertising services provider may share non-personally identifiable information that they have gathered about Web users and their interests with NAI member and other companies (such as advertisers, advertising agencies). However, if a user opts out of online behavioral advertising by an NAI member company, the user's data may not be shared with other companies for such purpose.

---

[2] For the 34 NAI member companies, it is difficult to address the privacy practices for each company comprehensively in response to these questions, and we have instead attempted to provide a general overview of practices. At its opt-out page (http://www.networkadvertising.org/managing/opt_out.asp#), the NAI provides a comprehensive directory of links to "More Information" from each member company, including descriptions of its privacy practices.

[3] The NAI's approach mirrors that recommended in the FTC's Self Regulatory Principles for Online Behavioral Advertising.

(d) As previously discussed, NAI members generally use cookie-related technologies to gather advertising-related data that is not associated with personally identifiable information at the time it is collected. In those instances in which personally identifiable information about a user is accessible to the NAI member company in conjunction with advertising-related data about the user, a variety of solutions may be deployed to de-identify the advertising-related data: such data may be immediately segregated from personally identifiable information at the point of collection, using discrete data systems and technologies; or alternatively, encryption technologies (such as one-way hashes) may be used to de-identify the advertising-related data. Some NAI member companies have established additional policies relating to the deletion after fixed periods of time of IP addresses and other potential unique identifiers, in order to provide additional assurance of the anonymity of user information.

(e) As discussed in response to question (1), the intended business purpose for the collection and sharing of online advertising information is to provide Web site visitors with more, rather than less, relevant advertising. At the same time, NAI member companies affirmatively minimize the amount of information necessary for this objective by using advertising technologies that leverage non-personally identifiable information, and by adhering to other standards and practices (such as those described above in response to sections (b) and (d)) intended to provide additional protection of advertising-related information about consumers.

(f) As previously discussed, the NAI requires that its members provide a consumer with an opportunity to exercise a choice to disallow online behavioral advertising with respect to a particular browser.

(g) As discussed in response to question (1), requiring a user's opt-in even to non-personally identifiable uses of cookies to improve ad relevance could pose a profound risk to both the user experience and the economic model for ad-supported Web services. This would significantly affect both Web publishers and the NAI member companies providing these publishers with advertising services. Faced with a potential barrage of opt-in prompts asking their permission to serve relevant ads, consumers might reject this approach entirely, uprooting the revenue model for most of today's Web offerings. There could also be new privacy challenges: Web sites could have significant incentives to start requiring that all their users furnish personally identifiable information, rather than allowing users to consume ad-supported content without registering.

4. **What percentage of your members' users know what information is collected about them and how that information is used?**

NAI members are required to provide notice of their collection and use practices on their own Web sites. NAI members must also require that the Web publishers for whom they provide online behavioral and other advertising services also disclose NAI members' practices on the publishers' own Web sites.

As previously discussed, NAI members generally provide online advertising services on a non-personally identifiable basis. Not knowing the identities of "users" of the Web publisher sites on which advertising-related data are gathered, NAI members do not have access to data relating to the specific knowledge of Web site users about NAI members' collection and use practices.

There have, however, been recent surveys reflecting general consumer awareness of data collection and use for online behavioral advertising. Consumer awareness of third party advertising practices has increased over time. A TRUSTe survey found that 71% of consumers are aware that their browsing information may be collected by a third party for advertising purposes. *See* TRUSTe, *2008 Study: Consumer Attitudes about Behavioral Targeting* (March 28, 2008), *available at* http://www.truste.com/pdf/TRUSTe_TNS_2008_BT%20_Study_Summary.pdf.

* * *

The NAI appreciates this opportunity to provide additional information.

Very truly yours,

Charles D. Curran
Executive Director

○