

Memorandum

TO:
IAB

FROM:
Venable LLP

RE:
Summary of FTC Behavioral Targeting Town Hall

DATE:
November 5, 2007

The Federal Trade Commission on November 1-2, 2007 conducted a two-day “town hall” on behavioral targeting online, *Behavioral Advertising: Tracking, Targeting, & Technology*. The busy schedule included nine panels composed of representatives from a number of leading online companies, government officials, and privacy advocates. Set forth below is a summary of the workshop.

The summary of day two’s proceedings begins on page 12.

Day One—November 1, 2007

FTC Chairman Majoras, through a videotape, welcomed everyone to the so-called “town-hall” on behavioral targeting.

Introductory Remarks—Lydia Parnes, Director, Bureau of Consumer Protection, FTC

Ms. Parnes stated that this workshop feels like “deja vu” in that these same issues were considered in a two-part workshop that the FTC held in 2000 on “online profiling.” She indicated that this workshop, like the one in 2000, would focus on the use of information about consumers to deliver targeted advertising online. She said that one reason that the FTC had convened this town hall is that the market has changed dramatically since the time of that workshop. She indicated that it is clear that these practices have become more prevalent in the marketplace and will be more widely used in the coming years to increase precision. She also noted that consolidation in the marketplace is a driver of increased focus on this industry.

Ms. Parnes said that this is the first in a series of town-hall meetings to grow out of last year’s *Protecting Consumers in the Next Tech-Ade* workshop. Ms. Parnes stated that there are clear benefits to

targeted advertisements, citing as an example the provision of advertisements for tennis rackets to a person interested in tennis. She then described the program for the day, noting that the panels would focus on four perspectives: (1) technology; (2) self-regulation; (3) privacy advocates; and (4) industry.

Session 1: Overview of Behavioral Targeting

This session was composed of four participants, one from each of the above-listed groups. The technology presentation was given by Richard Smith of **Boston Software Forensics**. Mr. Smith previously was a privacy advocate. He primarily described the mechanics of how Internet advertising works. He used the *Washington Post* as an example to describe online advertising. He demonstrated that there are 17 servers that provide content for one web page. He described cookies, web analytics, web publishers, web beacons, and the interplay between these components. He called the combination of these components the “ad targeting funnel,” describing how IP addresses, time of day, and other elements all result in producing banner advertisements. Mr. Smith described several models for online advertising:

- A search engine model with sponsored links similar to the offline yellow pages;
- A model where advertisements are all at the bottom of a page and triggered by keywords in the content or article in the web page;
- Geographic location-based targeting—he used as an example the fact that the Times of India is advertising US-only products such as Netflix, an indication that the website is advertising based on the location of the consumer;
- Demographics, using self-reported demographic data;
- Targeting consumers with ads such as Amazon does by suggesting products that others who had bought similar products also purchased;
- Addition of profiles and other databases tied to cookies, associating behavioral profiles with cookies; he described this as similar to traditional offline demographic segmentation that matches advertisements with certain pre-determined segments of the population.

Jeff Chester, executive director, **Center for Digital Democracy**, described his view that the way in which behavioral targeting and online advertising develops will have “profound” consequences for our democracy and expressed concern about whether there will be any consumer protection or privacy at all when this marketplace has fully developed. Mr. Chester indicated that his organization had filed a 50-page complaint with the FTC on these issues last year and that, in his view, it is time for the FTC to act to protect Americans. He described his view of abusive practices such as advertising Ritalin to children, or subprime mortgages to the indigent. He never connected how or why these concerns would be addressed in this context. He kept stating that just because behavioral targeting is permitted does not mean that it is right to engage in such practices. Mr. Chester said that today his organization filed an updated 76-page complaint against online advertising companies with the FTC.

Randall Rothenberg, president and CEO, **Interactive Advertising Bureau**, stated that IAB members' goal is to deliver the best products for consumers, indicating that self-regulation and market forces will provide the best regulatory framework for responsible business practices in this environment. He stated that advertising is the foundation for Internet content today. Behavioral targeting is responsible for lowering the cost of advertising and improving results. He described, contrary to the assertions of Mr. Chester, that the Internet, fueled by online advertising, has torn down barriers to entry in content and distribution, highlighting that never before has speech been more open and available. He emphasized the dramatic growth in the online advertising marketplace, measuring \$20 billion this year, with 32 million users alone having used online classified advertisements.

Trevor Hughes, executive director, **Network Advertising Initiative**, stated that "everything old is new again," indicating that targeted advertising to send materials to people likely to be customers has occurred since 1872 when Montgomery Ward mailed catalogs to those most interested in them. He indicated that there are a number of layers of protection online that have developed over the past 10 years. He said that the web is a great democratizing agent, with communities of interest that have never existed before. He emphasized that more than 85% of the Fortune 500 companies have posted privacy policies imposing obligations on the organization. He noted that a number of technological controls have been developed, including P3P controls, self-regulatory frameworks, seal programs, software, and privacy enabling tools. He emphasized that this is an ongoing dialogue and that NAI is continuing to look to improve solutions to complex issues.

Remarks—FTC Commissioner Jon Leibowitz

Commissioner Leibowitz remarked that consumers seem to understand and appreciate that Internet advertising supports the offering of free online content. He expressed concern, however, that consumers may be paying too high a price in terms of privacy for the benefits of the Internet. Commissioner Leibowitz noted that of particular concern to him is the practice of selling consumer profile information to third parties, the loss of anonymity through online searches, the potential risk of data breaches, and targeted ads based on communication transferred via VoIP services.

Commissioner Leibowitz stated that behavioral marketing is a complicated issue because the privacy trade-off associated with profiling may be acceptable to some individuals but not others. Discussing the fair information principles and their application in this context, he noted that although in theory consumer notice is good, many times privacy policies are posted inconspicuously, are written in legalese, and are in very small print.

The Commissioner also stated that he is particularly concerned about Internet advertisements targeting children, stating that behavioral targeting is reducing the parental buffer between marketers and children created by the Children's Online Privacy Protection Act (COPPA).

He suggested the following possible improvements and observations for the industry:

- standardized privacy policies and shorter notices, which consumers may more readily understand;

- more opt-in choices when it comes to consumer information, particularly when sharing such information with third parties;
- the industry default should be opt-in; and
- more competition on privacy issues.

The Commissioner indicated that the Do-Not-Track proposal noted above has promising possibilities. He also stated that he is hopeful that the industry can solve many of these issues on its own, but indicated that the FTC will continue to keep a watchful eye. If systematic abuses were to become present, he warned that the FTC would take action. Commissioner Leibowitz concluded by stating that the staff is reviewing the Google/DoubleClick merger expeditiously, and although competition is the key focus, the Commission will consider the privacy implications as well.

Session 2: Behavioral Advertising Today: Understanding the Business and Technology

Dave Morgan, founder, **Tacoda Inc.**, stated that consumers are running the show; it's all about consumers and they want content to be free. Currently, there are too many ads with too little relevance. Consumers do not want clutter and interruption of their online experience. The world of tomorrow will bring fewer, more relevant ads. Consumers only will accept ads that are meaningful to them. Privacy protection is a growing advantage—companies are taking steps to make privacy a competitive advantage.

Robert Gratchner, director of privacy, **AQuantive**, a subsidiary of Microsoft Corp., discussed the Atlas technology and how it serves ads. He also detailed the measures that the company is taking to protect privacy, stating that it: (1) is a founding member of the Network Advertising Initiative (NAI); (2) does not collect personal information; (3) provides an opt-out cookie; (4) does not provide benefit to advertisers based upon users' browsing history; and (5) complies with Microsoft's privacy principles for Live Search and Online Ad Targeting.

Michael Walrath, senior vice president, Marketing Products Division, **Yahoo! Inc.**, described the ways in which Yahoo! participates in behavioral targeting and the direct relationship between supply and demand with respect to advertising and the various models (e.g., direct relationship with consumer, ad network, and ad exchange). He defined behavior targeting as "displaying ads or content based on insights derived from past user activity." Mr. Walrath noted that 63% of online consumers say they pay more attention to ads that fit their specific interests and that 55% of online consumers say that ads that fit their interests improve or greatly improve their online experience (Ponemon Institute, April 2006). He discussed the value proposition, and what the consumer receives in exchange for behavior targeting, stating that the consumer benefits in the form of innovation and free content (e.g., new mail interface, free real-time text messaging service within email, Yahoo! and Windows Live Messenger interoperability, and phishing protection with eBay and PayPal). Mr. Walrath stated that Yahoo! takes trust seriously—trust improves the consumer's experience, as well as the products and services offered.

Tim Armstrong, president, advertising and commerce, North America, & vice president, **Google Inc.**, stated that user trust and loyalty is Google's focus. The company's competitive advantage is

relevancy, less ads, and higher consumer trust. Google's products and services are designed with a high level of transparency, minimal collection of personally identifiable information, and user choice. Google's business is based more on content than contextual searches. Discussing the pending DoubleClick merger, Mr. Armstrong stated that DoubleClick allows others to compete in the ad display platform business. It is important to remember that DoubleClick does not own the data it serves. He reiterated the commitment to privacy and trust, stating that these two ingredients are needed for a healthy Internet. Mr. Armstrong stated that: (1) Google would work with any group in an effort to promote privacy and consumer trust; (2) a continuum of practices helps companies promote privacy and trust; and (3) it is important to tread lightly in this area—there are tremendous benefits to targeted advertising that should not be discounted. The FTC should recognize this going forward.

Chanterria McGilbra, vice president, business and channel development, **Netmining**, provided a European perspective on these issues and how the differing approach to privacy in the EU (e.g., Europe's consent-based/opt-in model) impacts targeted advertising. She stated that in light of the EU Directive's requirements, her company needs to be more innovative about participation in this space. Contrasting the U.S. and EU approaches to privacy protection, she stated that under the EU Directive, generally speaking, there is permission-based data collection, informed opt-in with possible opt-out for certain collections, no IP address tracking, as well the need to comply with national legislation. In terms of impact on the business model, she indicated that cookie profiling of online visitors is anonymous; site-specific score-based individual profiling is anonymous or personal, and behavior-driven interaction is anonymous or personal. Ms. McGilbra stated that the company focuses on behavioral selling—through score-based profiling, one can determine primary, secondary and tertiary interests. She discussed case studies and the tremendous return on investment that her company is having, stating that it has seen a \$192 USD ROI for every \$1 USD spent on Netmining Solution. She stated that, thus, despite the differing approaches to privacy protection, Netmining's model is working.

Pam Horan, president, **Online Publishers Association**, cited a recent study indicating that consumers are drawn to free content. It is important to serve up a positive user experience—advertising and a positive user experience are inextricably intertwined. There is a real value exchanged, she said. Consumers expect to see ads in exchange for the information. Ms. Horan stated that for many OPA members, targeted and behavioral advertising are particularly effective methods to ensure that advertisers are reaching their desired audience and that users are being exposed to products and services that may be relevant and of value to them. She also stated that without advertising, many content providers would be unable to maintain their websites, devaluing the Internet and the user experience. Discussing an OPA survey, she highlighted the finding that the majority of consumers prefer to see more relevant ads. She stated that trust is critical, and that OPA members recognize and respect this, which is why all OPA members post privacy policies.

Mark Westlake, executive vice president, sales and content, **HowStuffWorks.com**, discussed the perspective of a small business, noting that behavioral targeting is cyclical: it results in greater revenue to the company, which means more and better content for consumers, which in turn means more value to consumers, which leads to more viewers, and then to more revenue again. His site has worked with Tacoda to compete with the bigger sites, extending their reach, which helps account for the site's success. Behavioral targeting is good for content development and provides a better user experience, Mr. Westlake stated. In discussing potential privacy concerns, he said that (1) users can control cookies, (2) the site anonymizes data; (3) the site's behavioral partners adhere to industry privacy policies (e.g.,

NAI); (4) the site makes sure that it is mindful of the user's experience (4) the site uses the data correctly; and (5) the site provides notice to all of its users (via a privacy policy).

Ralph Terkowitz, general partner, **ABS Capital Partners**, stated that targeting is not a new industry. Targeted advertising appeals to consumers because it enables publishers to deliver more effective advertising with fewer ads. He suggested that it is important to abandon the personally identifiable/non-personally identifiable data distinction. We need to allow consumers to be let alone, he said. Consumers need to be in control—there are instances in which they want targeted ads, and those in which they do not. There are new threats around targeting on the Internet, and new solutions possible since this is a new/different medium. The barrier to entry for bad actors is lower—it is cheaper to be a bad actor online, and there are no reputational constraints for these bad actors which help reign in corporate players. There should be a more sophisticated model of consumer choice. On the Internet, consumers are more empowered to make changes.

Carlos Jensen, assistant professor, School of Electrical Engineering & Computer Science, **Oregon State University**, represented the academic perspective, stating that the key issues are whether users are treated fairly and whether their privacy rights are protected. He discussed the iWatch web crawler and how it catalogues online data collection and privacy practices such as cookies, web bugs, pop-ups, banner ads, and privacy policies and seals. Mr. Jensen noted that the use of web bugs is growing in the U.S., but declining in the EU. He discussed a model of how information is shared over the Internet, noting that more than 1,700 servers are connected through 1,365 web bugs.

Highlights of Questions and Answers:

Making distinctions and serving ads accordingly. In response to a question concerning whether it is problematic for companies to make choices and serve certain ads to different individuals, Mr. Morgan of **Tacoda** stated that the “creep factor” test needs to be considered. He said he used the test about whether the particular ad would make his mother uncomfortable, citing areas that may not be appropriate for behavioral targeting, such as in the health and children's contexts. However, showing different ads to different people is what consumers want, and it is all about them.

Consumer access to information. Responding to the question of whether consumers can access information about them, Mr. Morgan of **Tacoda** stated that the competition is fierce on this issue. Companies are testing techniques so that consumers can access and change information maintained about them; for example, Weatherbug.com is testing opt-ins to certain information.

An opt-in model. There were discussions about whether an opt-in approach works in this context and how to motivate consumers to opt in. Such a model is used in Europe, and Ms. McGilbra of **Netmining**, a Brussels-based company, indicated that this does work. Mr. Morgan of **Tacoda** stated that there is less free content in Europe as a result of the opt-in model. It is not due to a lack of broadband or mobile penetration in Europe, rather the lack of the advertising revenue is the reason for less free content.

Content that is off limits? It was asked whether there are certain types of content that are off limits in terms of targeting, and how consumers know what these limits are. Related to this, there was a discussion about whether targeting is appropriate in the context of sensitive data, such as health and

children's information. Mr. Westlake of **HowStuffWorks.com** stated that the most important factor is consumer expectation. There are brand constraints that will help ensure that practices, although technologically possible, are not undertaken if they are not consistent with consumers' expectations.

Session 3: Consumer Survey Data

George R. Milne, associate professor of marketing, **University of Massachusetts-Amherst**, and Dr. Larry Ponemon, chairman and founder, **Ponemon Institute**, presented their findings from separate surveys regarding consumers' understanding of cookies and consumer preferences related to data collection and use. Prof. Milne reported the following trends identified from his research:

- Consumers want control of their information and their online environment (*e.g.*, 63.8% want to block pop-ups, while 34.5% prefer to opt in to receiving such ads);
- Consumers are concerned about new technologies used to acquire information and deliver advertisements (“Tech”);
- Consumer groups exist with very different online preferences on how to control specific technologies (*e.g.*, 45% of users do not want Tech used, 34.5% prefer an opt-in option, and 13% prefer an opt-out approach);
- Consumers have different expectations than both Marketing Managers and Direct Marketers; and
- Marketing Managers and Direct Marketers have different expectations; thus, all marketers are not the same.

Dr. Ponemon identified three categories of online consumers through his research: (1) privacy centric (8%), which includes users who are so deeply concerned about privacy issues that it affects their online behavior; (2) privacy sensitive (72%) users who care about privacy but do not want to be inconvenienced by the issue; and (3) privacy complacent (20%) users who are not generally concerned about online privacy. Dr. Ponemon presented the top three factors for building online trust with consumers. These factors include (1) the presence of an online privacy policy, (2) the frequency of ads received, and (3) a policy of not sharing personally identifiable information. Dr. Ponemon also provided the following trends identified from his research:

- Consumers want more control over the privacy of the information they share online with marketers;
- Consumers prefer personalization of advertisements when the ads are relevant to their interests or provide additional convenience;
- Consumers have a negative perception about the term “cookie,” the effect of which is to prevent consumers from engaging with a website after reading about cookies in the site's privacy policy;

- Only 48% of those users who understand the function of cookies are concerned about their use;
- 84% of users want control over the type and frequency of ads sent from a specific marketer;
- The longer a user has relationship with a website, the less likely that user will be to delete a cookie from that website; and
- Consumers are generally distrustful of online marketers and are taking steps to control cookies on their PCs. Permission is important to establishing trust and confidence in the online merchant.
- Trust leads to more and better personal information being shared by the consumers with the marketer or merchant.

Session 4: Data Collection, Use, and Protection

Nicole Wong, deputy general counsel, **Google Inc.**, stated that: (1) advertising is a critical component of the Web ecosystem; and (2) Google’s users’ trust and their privacy are critical to its business. Google’s goal, she said, is to provide the benefits of online advertising in a way that protects its users’ privacy. Google’s approach is to design privacy into its products. It uses contextual-based advertising—Google targets consumers based on the actions they take, and not on profiles. Google wants to identify what the user is looking for in a particular moment. It undertakes ad matching based on limited information. The user does not register, and the only information collected is standard log information (e.g., IP address, URL, time and date). Describing Google’s privacy protection measures, she stated that Google limits data used for ad targeting, limits disclosure, and protects against unauthorized access. She noted that as the online environment continues to evolve, it will be important to continue to evaluate these issues and tailor consumer protections.

Diane McDade, director, policy and implementation, trustworthy computing, **Microsoft Corp.**, stated that when Microsoft looks at privacy, it thinks about embedding it into the product—privacy by design. Describing its practices, Ms. McDade stated that Microsoft’s entire ad system is architected for privacy: the company does not utilize any information that directly and personally identifies an individual in the ad system. They make sure that all employees are aware of privacy issues, and confirm this through both internal and external audits. She stated that Microsoft’s privacy-enabled architecture gives customers the best of both worlds: to sign-in and authenticate when they are using personalized services, such as email, and to receive relevant targeted advertising based on information that does not directly or personally identify them. She discussed the acquisition of aQuantive and working with industry on the issues related to third-party ad serving building on the NAI principles. She also discussed continued investment in data security issues.

Scott Nelson, founder and chief operating officer, **TruEffect**, called for a change and removal of third-party from the third-party ad serving model. He also called for the elimination of cookie collection. He noted that consumers have “voted with their feet” and want an anti-adware environment. Mr. Nelson stated that the success of anti-spyware and anti-adware software has depleted the value of

anonymous cookie profiling databases. Looking toward the future, he stated that data about consumer behavior will not be stored in cookies.

Chris Kelly, chief privacy officer and head of global public policy, **Facebook**, discussed Facebook's approach, which he described as privacy by design. He noted that an important factor of the NAI principles is a clear distinction between personally identifiable and non-personally identifiable information. Facebook is offering a social utility to share information with confirmed friends. It offers real-time user control, with privacy settings (no settings reveal profiles to the world); users can share as much or as little information as they chose. The goal, Mr. Kelly said, is consumer empowerment. There are two key principles: (1) users should be in control; and (2) users should have access to information they want to share. The site undertakes advertising that is targeted based on information provided. He also discussed security measures, stating that key to protection is the fact that profiles are not widely available.

Amina Fuzlullah, staff attorney, **U.S. Public Interest Research Group**, stated that behavioral targeting raises serious concerns for consumers. She said that consumers give up information and that affects their choices and prices. She also questioned the distinction between personally identifiable information and non-personally identifiable information. She added that it does not take personally identifiable information to identify a person—a picture of a person can be put together through non-personally identifiable information. She expressed concern about how long data is kept, who will see it, and how it changes the consumer experience. Ms. Fuzlullah said that we need a uniform system, rather than a hodgepodge experience. She expressed concern about a lack of transparency and consumer control. Although the online environment has a good deal of benefits, the utility drops off with the amount of information taken.

Lisa Campbell, senior legal counsel, **Office of the Privacy Commissioner, Canada**, provided a comparative perspective with Canadian privacy laws and how these issues are being addressed in Canada. Discussing the application of the Canadian laws in the private sector, she stated that if the data can be associated with a person, it is personally identifiable and the Personal Information Protection and Electronic Documents Act (PIPEDA) applies. She noted that anonymity is important, and it is difficult to do. In terms of transborder data issues, under Canadian laws, it is required to inform consumers that their data will be available to law enforcement in other countries. She set forth three key principles: (1) consumer control over their own information; (2) who has access; and (3) expressive privacy (e.g., consequences of posting information, such as losing job).

Highlights of Questions and Answers

Data retention. Among the issues discussed was why Google and Microsoft moved toward shorter data retention periods. Ms. Wong of Google stated that there were three factors driving this decision to maintain log data only for 18 months: (1) ensuring the most robust system with respect to services (e.g., accuracy and assisting with search queries); (2) providing a definite time period for users; and (3) for security reasons and to prevent fraud and spam to Google's index. (e.g., to identify hackers or patterns of activity). Also, they need to retain data for record keeping purposes, such as tax auditing and compliance with the Sarbanes Oxley Act. Ms. McDade of Microsoft stated that in addition to the factors set forth by Google which have similarly impacted Microsoft's data retention, with respect to

security, it is useful to look at the data to protect future attacks. She also noted that Microsoft has decided that after 18 months it will remove all other identifiers other than IP addresses.

Merger of Google and DoubleClick and data merge. Ms. Wong of Google was asked how the DoubleClick data will be handled if the merger goes through. She stated that it is important to keep in mind that none of the data that DoubleClick has is owned by them. DoubleClick has no right to use the data in a non-aggregated, individualized form. If the merger is allowed to proceed, these obligations will float to Google.

FTC focus. The panelists were asked whether there are practices on which the FTC should focus. Ms. McDade of Microsoft stated that all sites should have privacy policies. She also stated that it will be important to ensure that there is no adverse consumer discrimination as a result of this targeting. There are outliers in every industry, she noted; they could undermine the behavior of all of the good actors. Mr. Kelly of Facebook stated that anything outwardly deceptive should be stopped. Ms. Wong stated that the biggest challenge is not conquering the bad, but whether the current approach is still right from a technological perspective.

Session 5: Roundtable Discussion of Data Collection, Use, and Protection

This session focused on the type of information collected, how long data is retained, how it is used in behavioral marketing, and whether consumers appreciate or understand information collection and use practices in the web ecosystem. The moderators' questions mostly involved potential harm arising from behavioral marketing, what actions should be taken, and by whom. Below are highlights of some of the comments made with respect to this concern.

- Declan McCullagh, chief political correspondent, **CNET News**, stated that he appreciates the potential for misconduct through the Internet, but believes that the tools need to combat misconduct and enforce existing laws exist.
- Dr. Larry Ponemon, chairman and founder, **Ponemon Institute**, expressed concern about the potential for a data security breach, available technology being used for illegal purposes, and that restrictions may harm invention on the Internet.
- Kathryn C. Montgomery, professor, School of Communication, **American University**, expressed concern for the vulnerable consumer segments where behavioral marketing could be used to prey on certain consumers. She encouraged some industry-wide standardization in practices, particularly transparency in information collection and use practices.
- Leslie Harris, executive director, **Center for Democracy & Technology**, identified the inappropriate use of technology as her greatest concern. She stated that she is less concerned about the use of data for advertising, and more worried that data and technology may be used for more harmful activities. She recommended empowering consumers with more choice, better education, and easier ways to elect preferences.

- Pam Dixon, founder and executive director, **World Privacy Forum**, expressed concern about the possibility that the information associated with a user may not accurately reflect a consumer’s preferences. Such conditions could result in the consumer being allocated to an incorrect segment, depriving that consumer of more relevant opportunities. She stated that this could lead to less than favorable loan terms or denial of service based on perceived eligibility.
- Richard Smith, **Boston Software Forensics**, stated that the issue of behavioral marketing is about fairness, and questioned whether consumers should give up privacy. He said that technology is the solution, but believes that the FTC could provide an opt-in regime for cookies.
- Chris Kelly, chief privacy officer and head of global public policy, **Facebook**, identified security of sensitive data as his primary concern.
- Amina Fuzlullah, staff attorney, **U.S. Public Interest Research Group**, stated her belief that consumers feel they do not control their online experience. She recommended that companies increase their transparency online with respect to their information practices. She urged companies to provide clear disclosure in terms that inform consumer as to how practices really affect them.
- Nicole Wong, deputy general counsel, **Google, Inc.**, commented that the greatest harm is the inappropriate collection or combination of information about a user or breach of security. She also stated that a business could create a harm if it served the wrong ads, does not target well, or serves ads in a way that offends users.
- Scott Nelson, founder and chief operating officer, **TruEffect**, stated his belief that the advertisers need to share in the responsibility for consumer privacy.

Day One Wrap-Up—Jessica Rich, Assistant Director, Division of Privacy and Identity Protection, Bureau of Consumer Protection, FTC

At the end of the day, Jessica Rich provided her view on the themes of the first day of the town hall:

- there are different privacy expectations among consumers;
- there are many different business models and different uses of information;
- consumers like personalization but may not understand trade offs;
- there is increasing competition by business on privacy;
- there is a need for transparency and data security; and
- there is certain sensitive information that is off limits for behavioral targeting.

Day Two—November 2, 2007

Welcome Remarks—Joel Winston, Associate Director, Division of Privacy and Identity Protection, Bureau of Consumer Protection, FTC

Joel Winston stated that day one of the workshop provided a useful groundwork regarding who uses behavioral targeting, how it works, and how information is used. He noted that the benefits described include free Internet content and reduced ad “clutter.” He also indicated that several concerns have been raised regarding lack of control by the user and regarding use of sensitive information. He added that there are data breach concerns.

Mr. Winston said that day two would focus on finding the right balance to preserve benefits while protecting privacy. He indicated that he hopes that there will be additional discussion on disclosures and how they could be made more effective. Also on the agenda for day two was discussion about what standards and practices exist now and the current regulatory environment, as well as what self-regulation and government action might be appropriate. Mr. Winston mentioned that there will be an FTC workshop in December regarding Social Security numbers, at which there also will be an important discussion regarding finding the right balance between beneficial uses and protection from abuses and identity theft.

Session 6: Disclosures to Consumers

This session focused on disclosures to consumers, addressing whether they can be made more effective and whether they work in this space. There were discussions surrounding whether new and emerging efforts to address notice and choice that companies have taken, such as eBay’s “adchoice label,” will work, and whether this concept or other types of symbols, color codes, or rating systems are useful. Also discussed was what, if any regulation, in this space is appropriate. Set forth below is an overview of the three presentations during this session, as well as highlights of the roundtable discussion.

A. Panelists’ Presentations

Lorrie Faith Cranor, Associate Research Professor, School of Computer Science and Department of Engineering & Public Policy, **Carnegie Mellon University**, stated that consumers care about privacy, but do not always take steps to protect it. She suggested that there are two factors at work: (1) people do not understand the privacy implications of their behavior, and (2) the cost of privacy is too high. Ms. Cranor said that privacy policies are written in legalese and require a college level education to understand. She shared the results of a study about notice that she had undertaken, which include that:

- even well-written policies are not well-liked and are difficult for consumers to use;
- layered notices (in their current format) do not appear to help much;

- people perceive long policies as slightly more trustworthy, but find information more quickly in short policies;
- experimental formats are not immediately intuitive; and
- it is not obvious how to get detailed information, such as where to find information in P3P hierarchy.

The results of her studies indicate that accessible privacy information affects consumer behavior, and that consumers are willing to pay for better privacy.

Declan McCullagh, Chief Political Correspondent, **CNET News**, conducted two studies regarding search engines and privacy. Among the questions asked of search engine companies were:

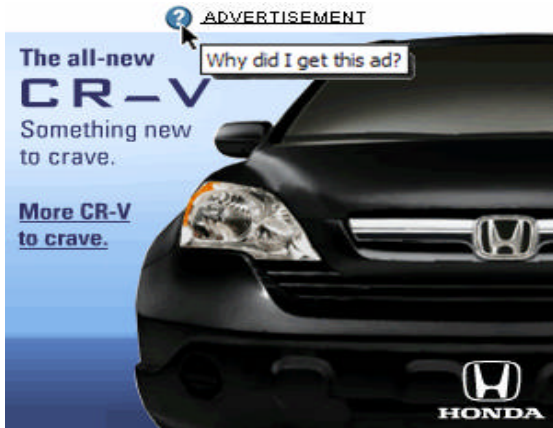
- What information is recorded about searches?
- Does the search engine store IP addresses linked to search terms and types of searches (image vs. Web)?
- Given a list of search terms, can the search engine produce a list of people who searched for that term, identified by IP address and/or cookie value?
- How long is data retained?
- If data is retained for a limited period of time, is it completely deleted (in such a way that the data and backups cannot be recovered, even under court order) or is it anonymized instead?

The answers to these questions varied by search engine, and determining which search engine is most privacy protective, Mr. McCullagh suggested, is a function of what issue is of most concern to consumers. For example, is anonymization more important than retention or whether the site engages in behavioral targeting? The results of this study are available at <http://tinyurl.com/356u3q>.

Scott R. Shipman, Chief Privacy Counsel, **eBay Inc.**, discussed some of the new measures with which the company is experimenting to address the issues of notice and choice in the ad context. Providing an overview of the company's practices with respect to disclosures, he highlighted the following four measures:

- posting of a Privacy Policy , which provides a summary of principles;
- eBay Preferences—notification and communication regarding preferences;
- advertisement notices—use of the phrase “Advertisement”; and
- advertisement choices—the AdChoice label.

eBay is developing an AdChoice label, which is a label to be placed near a graphical advertisement. The company is testing types of labels (what graphic, word, or option is best for their users), as well as placement. Below is an example of what eBay is testing:



The concept is that if consumers believe that customization is not appropriate for them, they can exercise this choice by opting out. The ad label would link to an AdChoice page, which describes the use of information for ad targeting and facilitates consumer opt-out. Following is another such example that is being tested:



Mr. Shipman stated that the key objective is to make the program known. The company will continue testing various formats to determine what consumers want and what works best for the eBay community.

B. Highlights of Roundtable Discussion

1. **Companies alerting consumers regarding ads.** It was asked whether companies alert consumers about ads.

Peter Cullen, general manager, trustworthy computing and chief privacy strategist, **Microsoft Corp.**, responded by stating that Microsoft has explored ways to provide information in context without burdening the consumer. He stated that different notices are needed for different scenarios. It is important to strike the right balance—on the one hand, they want to make sure that information is available and easily accessible, but on the other hand, they do not want to require consumers to scroll through 18 screens. He also discussed the importance of privacy policies in terms of the accountability that they offer—being accountable to consumers, consumer groups, and regulators.

Esther Dyson of **EDventure** stated that she does not believe that the FTC needs to set standards in this area; she believes the market is beginning to work. As evidence of marketplace solutions, she highlighted the Facebook model, stating that consumers are becoming accustomed to curating their own

profiles, and consumers will be more inclined to manage their interactions with marketers as a result of this phenomenon.

Srinija Srinivasan, vice president and editor-in-chief, **Yahoo! Inc.**, stated that the privacy policy is an outcome of a thoughtful process. Yahoo! has had its version of a layered notice for many years, with overarching principles and specific, additional disclosures for individual products. Also, she stated that there are implicit clues regarding use of advertising data, such as whether the site welcomes the user by name, which can tell users whether there is targeting and that their experience is being personalized. Ms. Srinivasan also stated that the presence and pervasiveness of a privacy policy is powerful and should not be underestimated.

Jane Horvath, senior privacy counsel, **Google Inc.**, discussed the ways in which Google is exploring different means of making practices clear to consumers, among these: (1) interactive blogs; (2) videos exploring privacy protections being posted on You Tube; and (3) launch of a privacy channel. Google uses increased notice where there is more actionable personally identifiable information, Ms. Horvath said.

2. Use of symbols or descriptive links which consumers can use to learn more about a site's practices. Joel Winston of the **FTC** asked whether sites could simply state near the ad something to the effect of, "We collect information about your activities and use it to serve ads of relevance to you. To learn more click here." He noted that the **FTC** has, in the past, looked at disclosures and found that a link without an explanation is generally ineffective. Consumers need to be drawn to it, he said. Related to this, it was asked whether some form of symbols or color codes could be used.

Mr. Shipman of **eBay** responded that the challenge of labels is that there are many permutations. Using a color-coded scheme to differentiate among, for example, anonymous data that is shared with an ad network, non-anonymized data shared with an ad network, and data that is sold, would generate a rainbow of colors. There is a value to white space on a Web page. Ms. Faith Cranor of **Carnegie Mellon** agreed that there are too many permutations, which would undermine the use of symbols. She stated that there is a role for the browser to make decisions for consumers. It can be programmed such that a consumer is only bothered when the site is "about to cross the line."

Mr. Cullen of **Microsoft** questioned how many little symbols would be needed—one for targeting, one for collection of social security numbers, one for disclosures to law enforcement—where would the line be drawn?

It was noted that the focus should not be on requiring people to read policies. Also discussed was the concept of "just in time" notices, which would give consumers a sense of warning when something surprising was going to happen.

3. Government regulation. Mr. Winston of the **FTC** questioned whether the government should step in. He noted that the panelists' silence seemed to convey that they did not think so.

Session 7: YouTube Contest Presentations

The Berkman Center for Internet and Society at Harvard Law School sponsored a video contest for which contestants submitted a two-minute video that describes cookies and their function. YouTube organized the competition and is hosting the videos on its website. The top five videos were presented at the town hall and served as a discussion piece for the panelists. At the end of the session, the winner, chosen by the panelists, was awarded a plaque and a check for \$5,000. Below is summary of the panelists' comments.

Esther Dyson of **EDventure** is credited with the video contest idea. She proposed the idea to draw attention to the fact that consumers do not understand how companies use cookies. She had expected a more negative depiction of the use of cookies. She commented that some consumers mistakenly believe that deleting cookies guarantees a user's privacy online.

Jeff Chester, executive director, **Center for Digital Democracy**, stated that he opposed the video contest because it placed the focus on cookies, while he perceives the problem involving the one-to-one marketing relationship used to engage consumers. Mr. Chester does not view technology as the problem; rather he is concerned with behavioral targeting. He also rejected claims that without Internet advertising there would be no editorial content. He argued that there is more available online than ad-supported content and that the Internet would not end without advertisements. In response to Ms. Dyson's question as to how the Internet could be funded, Mr. Chester responded that industry must make contributions to promote the availability of content. He warned that if industry continues to fund content that drives user behavior, interactive advertising will have an effect on the diversity of content.

Alissa Cooper, policy analyst, **Center for Democracy and Technology**, commented that while the videos did state that consumers are empowered to control cookies, there were inaccuracies as to the effectiveness of techniques and the implications associated with deleting cookies. She stated that consumers might not appreciate that clearing stored cookies also deletes opt-out elections. She also commented that users like ad-supported content, relevant advertisements, and control over setting online preferences.

Michael S. Zaneis, vice president, public policy, **Interactive Advertising Bureau**, described how online users are empowered to control how their information is collected and used. He explained that effective blocking tools, built into a user's web browser, are available to consumers that allow users to block unwanted cookies. This ability provides consumers with a personal choice as to what type of information they share; consumers are empowered by choice.

When asked about a consumer's role in deleting cookies, Lorrie Faith Cranor, associate research professor, School of Computer Science and Department of Engineering & Public Policy, **Carnegie Mellon University**, responded that web browser tools are useful for consumers in managing cookies. She noted Microsoft's decision to set the cookie default at blocking third-party cookies from companies without a privacy policy, but stated that improvement in the industry overall is needed. She commented that cookies are only part of the privacy problem.

Rob Pegoraro, personal technology columnist, **Washington Post**, commented that cookies are useful tools needed for the operation of the Internet. He stated that cookies are integral in capturing

consumer preferences, and that cookies are not nefarious objects that could lead to the introduction of spyware. He remarked that current technology, such as web browser settings, could be used to filter cookies.

Session 8: The Regulatory and Self-Regulatory Landscape

This panel was composed of leaders in the self-regulatory space and privacy advocates, and focused on whether existing frameworks are working and evaluated additional new frameworks. The panel began with three presentations, the first by Trevor Hughes who described the history and status of the **Network Advertising Initiative**. He picked up on themes from day one that demonstrate that consumers have a number of protections online including privacy policies, browser controls, P3P, and Safari. He indicated his belief that additional educational efforts are necessary, and that that would be a good place to focus efforts. He described the context in which the NAI was created and the success of its framework and subsequent activities over the years. He noted that there are 20,000 references to the NAI opt-out on privacy notices throughout the Internet. He emphasized the continued commitment of the IAB to review areas where the NAI principles can be revised.

Pam Dixon, founder and director, **World Privacy Forum**, described her belief that the NAI framework has failed and that consumers are not using the NAI opt-out cookie. She noted that this cookie is fragile and susceptible to deletion. She indicated that the recently announced AOL adoption of the Tacoda hardened cookie is an attempt to solve this problem. She indicated her belief that consumers do not understand the NAI cookie opt-out and are not using it. She added that NAI was set up for old technologies that are being used in new ways far beyond cookies. She indicated that new technologies, such as “flash cookies,” are outside of the NAI system, but raise the same issues. She also expressed concern about the fact that the NAI is limited in its scope of membership.

The third initial presentation in this panel was from Reijo Erik Aarnio, a **Data Protection Ombudsman for Finland**. He described how the EU laws apply to behavioral targeting.

A roundtable discussion followed these presentations. Mike Zaneis, vice president, public policy, **Interactive Advertising Bureau**, described IAB’s guidance for privacy practices online and the commitment of IAB to these important issues. He stated that IAB will continue to look at self-regulatory initiatives and enforcement tools. Jerry Cerasale, senior vice president, government affairs, Direct Marketing Association, described DMA’s long standing self-regulatory commitment to privacy. He explained that DMA members are bound by DMA guidelines, and that DMA has effective policing through its ethics committee with the goal of bringing companies into compliance. Mike Hintze, associate general counsel, legal and corporate affairs, **Microsoft Corp.**, noted that there is no silver bullet preferred means of providing choice to consumers, and described that there are a lot of ideas in the marketplace.

Ari Schwartz, deputy director, **Center for Democracy and Technology**, expressed concern that a number of companies do not follow guidelines and are not offering opt-outs or user control. He cited an Annenberg/Berkeley study that supports this point. Jessica Rich of the FTC asked whether there is a model other than notice and user choice that would be more effective in matching consumer preferences. She queried the possibility of implementing a harm-based model, where targeting of certain types of

advertisements would not be permitted. Mr. Schwartz suggested a framework where user controls are universal in coverage and technology neutral. Jeff Chester, executive director, **Center for Digital Democracy**, indicated that certain practices should not be permitted at all, such as certain advertising to children. Mr. Zaneis noted that there is a harm-based model that works in Section 5 of the Federal Trade Commission Act. He expressed that Section 5 allows for targeting those entities that are causing harm, and stated that this is not the “Wild West.”

Mark Cooper, director of research, **Consumer Federation of America**, expressed his view that self-regulation is not working, quoting numbers from earlier in the workshop that 99% of privacy statements are not acceptable. He indicated that there is a gap between what consumers expect and what they deserve. Ms. Dixon indicated that the NAI model does not work. Peter Swire of **Ohio State University** stated that we are now in the place online that we thought we prevented in 2000 when the NAI principles were developed. He stated that the goal is to have workable privacy preferences. He indicated that to get an appropriate result takes leadership, and that government should have done something sooner. Mr. Cerasale stated that if you listened to this panel, you would think that the Internet has been a failure and that consumers do not have confidence in the Internet, which clearly is not the case. He emphasized that DMA has a long-standing principle, that has worked well, that marketing data should only be used for marketing purposes.

A discussion ensued regarding a proposal offered by privacy advocates to create a Do-Not-Track List. This proposal would require advertising entities that place “persistent tracking technologies on consumers’ computers to register with the FTC all domain names of the servers involved in such activities.” The FTC would make this list available to consumers. The theory of this initiative is that consumers would then download the list onto their computers in a way that would stop behavioral targeting technologies. Mr. Cerasale expressed concern that such a system likely would limit the vast benefits of free content on the Internet. Mr. Zaneis indicated that such a proposal could render large parts of the Internet non-operational.

Session 9: Roundtable on the Future of Behavioral Advertising

This panel included discussions of future technologies that will enable behavioral targeting, as well as some of the current tools, such as those offered by Symantec (*e.g.*, Browser Defender and Identity Safe) to protect consumers against emerging threats.

Katherine Albrecht, director, **CASPIAN** discussed future tracking technologies, focusing on Radio Frequency Identification (RFID)—unique ID numbers that are remotely readable through purses, pockets, etc. She discussed RFID applications on mobile phones in Japan (Japan tested real-world cookies), loyalty cards, passports, to assign a value to consumers as they enter retail stores, as well as future plans to use the technology in connection with offering bank patrons differential treatment, on billboards to target people and to scan tags in garbage (to determine how quickly people consume particular products). Ms. Albrecht stated that this is extraordinarily harmful to consumers.

Mozelle Thompson, CEO, **Thompson Strategic Consulting**, stated that there is a lingering, but incorrect, impression that the public is dumb; they may be misinformed or uninformed, but they make choices about privacy. He noted that there still is a gap between what consumers and users know and

what they need to know. Although Web sites, public interest groups, and the government are doing a good job of informing consumers about privacy, there are more opportunities to provide information. Importantly, he cautioned, the FTC's role is not to take action without clear harms. Commissioner Thompson opined that there is much room for innovation. Innovative tools that inform consumers and users what companies do with information are being developed. We are seeing more consumers flock to those companies—they represent trust between consumer and vendor, he said. Commissioner Thompson also noted that the primary risks to consumers are not posed by those companies in the room.

Highlights of Questions and Answers

Will alternatives to cookies to emerge? Responding to this question, Jules Polonetsky of AOL stated that cookies are not perfect. The disadvantage of cookies and their limits is actually a real advantage. It is important to get the cookie structure correct, he said. Alissa Cooper of CDT stated that the emerging threat lies with the ISP partnership with the ad network. The ISP has visibility into everything—no one knows more about the consumer than the ISP and, thus, a partnership with an ad network could create a very rich profile. Mr. Thompson of **Thompson Strategic Consulting** stated that if it was not cookies, it will be another technology. There is a demand for mass customization and consumers want real-time delivery.

Legal and business questions surrounding ISP model and tracking. Joseph DeMarco of **DeVore and DeMarco, LLP**, a former prosecutor, stated that behavioral targeting can raise questions of wiretapping, hacking/computer fraud, and intellectual property issues. As complex as notice and consent issues are, he said, the legal analysis and permission is even more difficult when the issue concerns the provider of the pipe. Analysis of data flows by ISPs immediately raises wiretapping issues. There is a question as to what is context, which will be important to address. Turning on cookies that have been disabled raises hacking issues and implicates computer fraud laws. Mr. De Marco stated that there also are copyright issues if there is modification of a site through ad delivery (e.g., ad blockers).

Social network sites—are there unique considerations in this context? Responding to this issue, Mr. Thompson (who has represented Facebook) reminded the group that not all social networking sites are the same. Social networking sites provide more granularities in terms of privacy, he said. They represent the new privacy model. People want to send out information, but they also want to control who has access. Mr. Thompson stated that this is not a binary equation of ad or no ad—rather, the issue is an ad to whom and from whom. He noted that the ad process will not be top-down only in the future. Users will receive ads and information from their neighbors and friends as well.

Trust but verify—how can we encourage trust? John Thorne of **Verizon** stated that consumers respond to different levels of privacy. He provided examples of how customers voted with their feet and joined Verizon in the wake of other companies' proposals to make available a cell phone directory, as well as ISPs' practices in connection with responding to subpoenas. He stated that privacy is important and that consumers distinguish among companies based on privacy. Mr. Thompson stated that it is difficult to pursue bad actors. The real challenge, he said, will be to create a race to the top because businesses find it easier to deal with mediocrity.

Closing Remarks—Eileen Harrington, Deputy Director, Bureau of Consumer Protection, FTC

Summing up the town hall discussions, Ms. Harrington of the **FTC** made the following observations:

- (1) Behavioral advertising is a growing practice that is largely invisible;
- (2) There is general agreement that greater transparency and control is needed;
- (3) There are legitimate concerns about what happens to information. Among these concerns are secondary uses of information and data security issues, particularly where sensitive data is involved.
- (4) The FTC wants a reasonable approach, which is flexible, provides consumers with control, prevents harm and creates greater accountability.

She discussed some of the promising ideas, which include a Do-Not-Track List, updates to the NAI principles, and better consumer education. Ms. Harrington indicated that the FTC has not seen enough of the facts surrounding information collection for behavioral targeting. She also stated that there is a lack of concrete suggestions about improving consumer protections. Finally, she stated that the FTC will continue to ask questions about these issues.