

# Behavior Targeting and the Modeling of Economic Compensation for Accessing Private User Behavior Information.

Daniel O. Rice

*Technology Solutions Experts, Inc.*

**Abstract**— Behavioral targeting uses web technologies to gather web browsing information that when analyzed is used to tailor direct marketing efforts at specific potential customers or groups of customers. The use of 3rd party cookies in this manner, however, has been called “behavioral targeting” and many believe that it is an invasion of personal privacy. Organizations and businesses who engage in behavior targeting usually do it surreptitiously, without the individuals’ permission, and with the cooperation of the users’ Internet Service Providers (ISPs). This ongoing research proposes a simple solution that will allow informed users to participate in the collection and reselling of their own personal information including compensation to users for allowing their browsing behavior and personal information to be tracked. The market premise is that there is extreme value created by firms who track, analyze, and sell Internet users’ browsing activity. Businesses, such as marketing firms like DoubleClick, will be willing to pay for that information supporting compensation to users and ISPs. The technologies and economic foundations exist to support the functioning of an information market sustained by existing demand as well as the voluntary individual and ISP participation.

**Index Terms**— Behavioral targeting, behavioral advertising, direct marketing, 3rd party cookies, personal privacy

## I. INTRODUCTION

BEHAVIOR targeting is a recent version of customer profiling which is becoming popular with some online advertising firms through cooperative efforts with internet service providers (ISPs). This sometimes furtive advertising method uses 3rd party cookies to collect information about users as they browse the internet and click through hyperlinks<sup>1</sup>. The intended use of 1st party cookies, small files created and stored by the web browsers, was to allow functionality enhancing the browsing or commerce experience of browser users. More recently, 3rd party cookies have been used by web advertising companies, such as DoubleClick, to track behavior on the internet – these 3rd party cookies were simple to implement by inserting a graphics image (often a one by one clear pixel) on a webpage. The image links to a server controlled by a 3rd party advertising company that would serve up the graphics image and add or update the associated

cookie file in the web browsers cookie folder whenever the image is retrieved.

Behavior targeting entails the cooperation of the ISP; in some cases the ISP even allows a 3rd party to intercept and alter web traffic to users. Early tests of this practice, some rather alarming, have been pursued as early as 2006 in the United Kingdom when British Telephone allowed a 3rd party ISP to install equipment for the interception of their users’ web traffic without informing their users. [3] [4]

Informed individuals often provide personal information in the course of routine interactions with various organizations in order to conduct business or to receive service. [16] The exchange of such information is vitally important for most organizations, especially advertisers, and it also may have some significant benefits for individuals as well. Naturally, an organization may require information in the course of providing goods and services to individuals and these individuals may receive better service by truthfully revealing personal information. For instance, a patient may be asked by a doctor to report the average number of alcoholic beverages they consume in a week. The doctor then has information that may allow her to make a better diagnosis. However, through this process individuals may also expose themselves to threats of abuse of their personal information. An abuse of particular interest is the release and use of personal data for purposes other than the original intended purpose (i.e. suppose the doctor provides the above information to a beverage company or even to the patient's insurance provider). Individuals’ perceptions about the threat of abuse are significant, in fact a large percentage of the population are concerned and believe that they have lost all control of their personal information. [7]

## II. RIGHT TARGETING FOR ONLINE MARKETING

Behavior targeting provides a solution to a very important set of marketing problems; namely these problems involve the narrowing down of a population into a target list of individuals whom are most likely to respond to target marketing. Solving this problem often will reduce the cost of advertising in direct marketing because the individuals are likely to be more responsive to the advertising, reduce the social cost of bombarding individuals who are unlikely to purchase products and services with advertisements, and increase the benefit by getting the right information to those who are interested and likely to buy (most of us don’t mind when Amazon.com is able to give a good book recommendation, or a special offer on something that interests us).

<sup>1</sup> 3<sup>rd</sup> party cookies are small files recorded by the web browser pursuant to the visiting of a website, the original intention of cookies was that cookies would allow the browser to identify a returning user and ‘remember’ certain user characteristics and enable certain functions such as shopping carts that remember what is in the cart as a user goes from page to page in an online shopping environment).

The two essential elements of direct marketing on the Internet are (1) finding the right target market segment, and (2) getting the right advertisement to that segment. Behavior profiling helps in both of these arenas. There are a few typical information elements about users that online advertising firms would like to and usually do quite easily track online. [8] These include:

- visitor profiles gathered from site registration, age, gender, income, business data, etc. ;
- area of content a visitor is viewing starting with the first visit, systems automatically start learning about each site visitor's individual interests and tastes, they keep learning more with each repeat visit;
- Internet-based registration domain type, browser type, ISP, platform, time of day, day. of the week;
- key-word or key-phrase searches;
- demographic data IP address, high-level and specific domain;
- geographic data country, state, zip code, area. code;
- IP address and cookie information for ad or page;
- cumulative history of exposures to all ads in a campaign.

When online advertisers are not able to get these key pieces of information, they may resort to other means. Behavior targeting is one of these that necessarily involves the corporation of the internet service providers (ISPs) and is often done without the knowledge of the ISP user. Behavioral targeting of this type involves the surreptitious collection and analysis of personal information. Privacy advocates, watch guard groups, and now federal regulating bodies like the Federal Trade Commission (FTC) are becoming alarmed to this practice. [1] Some of these privacy concerns are discussed further in the following section.

### III. PRIVACY CONCERNS

The concern over privacy has so alarmed public advocacy groups that they have even made requests to the president that he should appoint a privacy czar. The White House responded by at least calling privacy a "top priority." [5] The federal government has been investigating various options to ensure the preservation of the privacy rights of its citizens in the information age. For example, the U.S Department of Commerce has issued several reports on privacy. [10][11][16] Still, the federal government is reluctant to become too involved in the regulation of information markets dealing in individuals' personal information. Regulation would be costly and may overly restrict the free exchange of information that is necessary for market efficiencies. Discussions of self-regulation of markets that deal in personal information are on the forefront of the debate. [11] Still, recent surveys reveal that little has changed over the past several years and the majority of individuals are still very concerned about their privacy. [6][7][13] "Online trust issues continue to impact consumer behavior on the Internet", states Fran Meier executive director and president of TRUSTe, when referring to a recent survey concerning online privacy by TRUSTe/TNS. Meier goes on to

add "high profile privacy breaches this year have exacerbated consumer concern." Still, it appears that little has been done by organizations, including the U.S. government, to safeguard citizens' privacy. [13]

### IV. A SIMPLE SOLUTION - COMPENSATING USERS THROUGH A BEHAVIOR TARGETING INFORMATION MARKET

One simple step in improving privacy is for third party advertisers or the ISPs to compensate users for voluntarily allowing behavioral profiling. The same mechanisms that enable third party cookies and the tracking of individuals on the Internet could be used to enable the compensation to individual users. The economic foundations for self-regulating the buying and selling personal information using a market mechanism have been developing over the past several years. [9][16]

As an example of how this market might function, consider the collection of a user's web browsing behavior when visiting an internet site for creation of actionable marketing information and analysis. Quite fortunately, the architects of the internet have created the perfect protocol this type of web browsing behavior and information tracking with the Hypertext Transfer Protocol (HTTP)<sup>2</sup> which enables the explicit tracking of this type of information using the Uniform Resource Locator (URL). The Web uses URLs to provide unique addressing so that a user's web browser can retrieve files from locations such as the URL;

<http://www.getstuffforless.net>

which, when typed into a web browser's address line will retrieve the associated document from the server that resides at that URL. The fact that an individual is looking at the Get Stuff for Less website has value to several parties including 3rd party marketers and perhaps the Get Stuff for Less retailer. It is likely that information of additional value could be derived from a 3rd party knowing exactly what topics, articles, and information that user accesses information at the Get Stuff for Less website.

For instance, knowing that a user has clicked through to more detailed URL, such as,

<http://www.getstuffforless.net/watches/>

on the Get Stuff for Less website, is much more revealing and perhaps very valuable. In fact, marketing and advertising firms conduct extensive data analysis on exactly that type of information to leverage the knowledge that users visiting URLs like, <http://www.getstuffforless.net/watches/>, may just be interested in watches.

More detailed URL information such as,

<sup>2</sup> HTTP is an application-level protocol "for distributed, collaborative, hypermedia information systems." HTTP has been in use enabling the World Wide Web (WWW) global information initiative since 1990 (please see <http://www.w3.org/> for more information on the subject)

<http://www.getstuffforless.net/watches/designer/gold>

shows that a user has accessed even more specific information and may reveal more specific preference information about that user's interests; that is, that they are not only interested in watches, but in "high end" gold designer watches. The more specific the information about what users are looking for online the more the more valuable it is likely to be to a 3rd party online marketing firm or retailer.

Ideally, the mechanism would provide increased levels of compensation for increases in the revelation of information (that is, the information that a user visits the Get Stuff for Less website requires lower compensation than the additional information that the user looked at gold designer watches on the site). Ideally, a variable pricing mechanism could accomplish this. A simple compensation mechanism would provide an initial compensation for allowing knowledge of visiting a particular web site on the "home" level, and then could provide more compensation for each additional level where the "level" is the depth of the web browsing,

for example, [http://home/level\\_1/level\\_2/.../level\\_N](http://home/level_1/level_2/.../level_N).

Each individual then could chose whether or not they'd like to participate where participating users could receive compensation perhaps in the form of a flat price reduction in their cost of internet access (from the ISP). Next, they could determine if and to what level of detail the 3rd party should be allowed to track them which would result in a variable compensation depending on how much information the 3rd party is allowed to glean from users' web activity.

## V. INCENTIVES FOR MARKET PARTICIPATION

The goal of economic compensation model is to design a system that captures the value a 3rd party online marketing firm would place on this type of web browsing information and then design a mechanism for 3rd party to compensation to the individual users producing the data. A successful mechanism in the online marketing environment will require that: (1) the 3rd party marketing firm deriving value from collecting browsing information; (2) the users are willing to allow for this practice for compensation; and (3) the compensation mechanism is fair and secure.

The compensation model is only viable if sufficient market incentive exists to ensure market participation. It's been shown, and is generally accepted, that with appropriate compensation and assurance that personal information will not be abused, many individuals are willing to allow their personal information to be used for marketing purposes. [2] However, implementation of the compensation model should be careful not to reinforce the tendency some individuals may have to cheat or "game" the system by prolific strategic browsing simply to increase personal revenue. One possibility to govern cheating behavior would be setting a compensation limit, either daily or monthly, based on the normal or expected usage rate.

Although this simple solution may not eliminate cheating, it should at least mitigate the impact of intentional abuse by

cheaters and will avoid the problem of wildly overcompensating cheaters. More elaborate anti-cheating devices may also be employed such as anomaly detection technologies that can be used to ensure that browsing data collected is reasonable (discussion of these technologies are beyond the scope of this paper). Then if cheating is detected, the data derived from obvious abuse can be removed, and the user can be removed from the market. Ultimately we should realize that some of the information collected by 3<sup>rd</sup> parties may not be an entirely accurate representation of genuine browsing behavior. This is true of much of the real marketing behavior data collected using various devices including surveys, registrations, and other techniques. In this case the analysts may have to rely on analytics, statistical analysis, and data-mining tools to help sift through good and bad data. Also, in cases when a user does not want to be tracked they should have the option to turn off the tracking (a luxury currently not afforded by the behavior targeting techniques). Finally, we are optimistic that most users will be incentivized to trade their genuine browsing behavior for compensation.

Next, both the internet service providers (ISPs) and the 3<sup>rd</sup> party marketing information firms have economic and legal pressure to participate in the self-regulation of behavioral targeting based marketing. [11][13] The economic incentive to participate in the collection and sale of behavior marketing information is clear – there is a strong demand for these products and participation can add significant revenue to both ISPs and 3<sup>rd</sup> parties. The incentive to self-regulate is strong and getting stronger. Recently "the F.T.C. revised its suggestions for behavioral advertising rules for the industry, proposing, among other measures, that sites disclose when they are participating in behavioral advertising and obtain consumers' permission to do so." In fact, in the same article it is reported that the FTC commissioner, Jon Leibowitz, warned that "if the industry did not respond, intervention would be next." As has been the case in the past, it is likely that the marketing industry will enthusiastically find ways to self-regulate in order to avoid forced regulation. [1]

## VI. THE ECONOMICS OF BUYING AND SELLING PERSONAL INFORMATION

The rise of Internet commerce has greatly changed the application of economics to business commerce and part of this involves the economics of information privacy. Historically, information systems and computer science research have taken a rather technical view of privacy where privacy is reduced to a security issue. On the other hand, many modern economists have taken a different view of privacy. These economists view privacy as the voluntary exchange of individuals' personal information between parties. For instance, Hal Varian gives a simple example that shows how personal information could be used in economic transactions and points out that there are advantages to making personal information available. [14][15][16] It is mutually advantageous for sellers and buyers if the sellers are allowed to know some personal information about buyers such as what the buyer intends to buy. The benefit of this flow of information is most obviously the seller's discovery of

information enabling for the delivery of an appropriate product.

However, if a seller decides to pass the private information on to a 3rd party negative externalities may exist. The perceived invasion of privacy has a cost. Therefore, Varian suggests that a contractual agreement between individuals and the 3rd party. He illustrates this agreement using a simple example where an individual is offered a contract from the information seeker at the point of data collection such as "Check here if you would like your name distributed to other parties who will provide you with information about computer peripherals until 12/31/98. After that, name and address information will be destroyed. In exchange you will be paid \$5.00 for each list to whom your name and address is distributed." [12] [16]

Contractual agreements like this show an economic transaction which stipulates the right to use personal information and compensation to the individual each time the information is sold. Laudon develops this concept further in his National Information Market (NIM) concept. [9] The NIM illustrates a market where personal information is bought and sold by institutions. Businesses collect and process personal information reselling as an information product. Purchasers of the information may use it for commercial purposes over a defined period of time. Contributors of personal information are compensated each time the information is used or sold. This market functions much as the banking industry. The marketplace allows for a complete computer-based audit trail mitigating the risk of information abuse.

Laudon's NIM is a hypothetical market that illustrates how personal information could be bought and sold in a market setting. One important factor to consider when considering the trade of personal information goods is the pricing. Information goods cost structure is very different than many other products. There are typically large setup and collection costs and then each additional item costs comparatively very little. Varian explains the pricing these goods on cost makes little sense, and recommends pricing information goods based on value. [14] This would also support situations where different consumers have different values for the information product. [14] The issue of pricing these products would be of concern for the 3rd party firms collecting and reselling behavioral profiles. An overall market solution should consider all of these cost and pricing issues and will be the topic of future work in this area.

## VII. A COMPENSATION MODEL FOR 3RD PARTY COMPENSATION TO ISPS AND INTERNET USERS

A compensation model is used to incentivize (1) 3rd parties who are willing to pay for better web browsing information; (2) ISPs who are willing to sell user/individuals web browsing information; and (3) users/individuals who are willing to be compensated for the collection and sale of web browsing information. This compensation model illustrates the concept of how ISPs and users would be compensated by a 3rd party. The 3rd party total compensation,  $C_t$ , which is the total amount of payment they will make to the ISP and individuals who are providing personal information is:

$$C_t = C_{ISP} + C_{user} = C_{ISP} + w \sum_{u \in U} \sum_{s \in S} d_{us} \ell_s$$

where;

- $C_{ISP}$  - is the compensation the 3<sup>rd</sup> party makes to the ISP
- $u \in U$  - represents a user  $u$  who is a member of the set of all internet users,  $U$ , who visit internet sites through the ISP
- $\sum_{u \in U} \sum_{s \in S} d_{us} \ell_s$  - is the sum over all users, a cost of compensation for a compensation base of  $d_{us}$ , the compensation coefficient for user  $u$  visiting site  $s$ , and  $\ell_s$  the compensation for revealing that the user retrieved the level  $\ell$  of site  $s$ .
- $w$  - is a scaling factor

The above formulation shows an approach to begin modeling the compensation of users and the ISPs for access to personal information related to web browsing activity. Continuing research will include the application of this model in simulation by applying existing data sets about user web browsing behavior.

## VIII. CONCLUSION AND ONGOING RESEARCH

Behavioral targeting is a recent phenomenon that takes advantage of web technologies in order to better tailor direct marketing efforts increasing the cost efficiency of online marketing methods. However, many consider the use of 3rd party cookies for behavioral targeting as an invasion of personal privacy because the agencies engaged in this practice are doing it surreptitiously and with the cooperation of the users' ISP, but without the knowledge of the users. A simple solution is to inform the users and allow them to participate in the collection and reselling of their own personal information by compensating them. Obviously, enough value is created through this activity to support this type of compensation and the technology exists to enable a functioning information market.

Future research in this area will delve into the details an information market and compensation mechanism for behavioral targeting. The next opportunity in this research lies in the specification of a market mechanism and the analytical study of the market mechanism that demonstrate conditions under which social welfare is increased. This future research may be accomplished in several ways including either a

designed economic experiment, quasi-experiment, or through simulation and numerical experience.

## REFERENCES

- [1] P. Boutin. (2009, Mar. 18). Survey: Online privacy is your problem, not DoubleClick's. *The Industry Standard* [Online]. Available: <http://www.itworld.com/internet/64534/survey-online-privacy-your-problem-not-doubleclicks>
- [2] A-N. Chang, P.K. Kannan, and A.B. Whinston. "The economics of freebies in exchange for consumer information on the Internet: an exploratory study," *International Journal of Electronic Commerce*, vol. 4, no. 1, pp. 85-102, Sept. 1999.
- [3] M. Kassner. (2008, Jul. 31). Behavior targeting: What You Need to Know. *Tech Republic* [Online]. Available: <http://blogs.techrepublic.com.com/networking/?p=612>
- [4] S. Gibson and L. LaPorte. (2008, Jul. 3). Security Now Podcast Episode #151, Phracking Phorm. *Gibson Research Corporation* [Online]. Available: <http://www.grc.com/sn/sn-151.txt>, August 25, 2008.
- [5] P. Greenberg. (2001, May 8). Internet Privacy: Back to Basics. *E-Commerce Times* [Online]. Available: <http://www.ecommercetimes.com/story/9473.html>.
- [6] Louis Harris and Associates and A. Westin. "Consumer Privacy Survey," Harris-Equifax, Atlanta, GA, 1995.
- [7] Harris Interactive Poll, Privacy On and Off the Internet: What Consumers Want, <http://www.harrisinteractive.com/news>, February 20, 2002.
- [8] G.G. Karuga, A.M. Khraban, S.K. Nair, and D.O. Rice. "AdPalette: an algorithm for customizing online advertisements on the fly," *Decision Support Systems*, vol. 32, no. 2, pp. 85-106, Dec. 2001.
- [9] K. Laudon. "Markets and privacy," *Communications of the ACM*, vol. 39, no. 9, pp. 92-104, Sept. 1996.
- [10] "Privacy and the NII: Safeguarding Telecommunications-Related Personal Information," *U.S. Department of Commerce*, Oct. 1995. Available: <http://www.ntia.doc.gov/ntiahome/privwhitepaper.html>
- [1] "Privacy and Self-regulation in the Information Age," *U.S. Department of Commerce*. Available: [http://www.ntia.doc.gov/reports/privacy/privacy\\_rpt.htm](http://www.ntia.doc.gov/reports/privacy/privacy_rpt.htm)
- [2] H.R. Varian. "Pricing Information Goods," presented at the Research Libraries Group Symposium Symposium on "Scholarship in the New Information Environment" held at Harvard Law School, Cambridge, MA, 1995. Available: <http://www.sims.berkeley.edu/~hal/Papers/price-info-goods.pdf>
- [3] "Consumers Have False Sense of Security About Online Privacy – Actions Inconsistent with Attitudes," *TRUSTe/TNS Privacy Survey*, Dec. 2006. Available: [http://www.truste.org/about/press\\_release/12\\_06\\_06.php](http://www.truste.org/about/press_release/12_06_06.php)
- [4] H.R. Varian. "Versioning Information Goods," Digital Information and Intellectual Property, Harvard University, Cambridge, MA, 1997. Available: <http://www.sims.berkeley.edu/~hal/Papers/version.pdf>
- [5] H.R. Varian. "Differential Pricing and Efficiency," *First Monday* [Online], vol. 1, no. 2, 1996. Available: <http://131.193.153.231/www/issues/issue2/different/>
- [6] H.R. Varian. "Economic Aspects of Personal Privacy," *Privacy and Self-Regulation in the Information Age*, Department of Commerce. Available: [http://www.ntia.doc.gov/reports/privacy/privacy\\_rpt.htm](http://www.ntia.doc.gov/reports/privacy/privacy_rpt.htm)